INSTITUTE FOR DEFENSE ANALYSES

A State Cyber Hub Operations Framework

Laura A. Odell, *Project Leader*

Cameron E. DePuy
J. Corbin Fauntleroy
Andrew S. Ferguson
Robert M. Rolfe

June 2016

Approved for public release; distribution is unlimited.

IDA Non-Standard Document
NS D-8008
Log: H 2016-000625
Copy

INSTITUTE FOR DEFENSE ANALYSES
4850 Mark Center Drive
Alexandria, Virginia 22311-1882

The Institute for Defense Analyses is a non-profit corporation that operates three federally funded research and development centers to provide objective analyses of national security issues, particularly those requiring scientific and technical expertise, and conduct related research on other national challenges.

About This Publication

This work was conducted by the Institute for Defense Analyses (IDA) under contract HQ0034-14-D-0001, Task BK-5-3889, "Creating an Affordable Strategy for Policy Issuance and Buying Power for the DoD CIO," for Principal Director/Director Analytics, Office of the Secretary of Defense, Chief Information Officer. The views, opinions, and findings should not be construed as representing the official position of either the Department of Defense or the sponsoring organization.

Acknowledgments
Andrew Wan, Jemakai N. Blyden Copyright Notice

Copyright Notice

© 2016 Institute for Defense Analyses
4850 Mark Center Drive, Alexandria, Virginia 22311-1882 • (703) 845-2000.

This material may be reproduced by or for the U.S. Government pursuant to the copyright license under the clause at DFARS 252.227-7013 (a)(16) [Jun 2013].

INSTITUTE FOR DEFENSE ANALYSES

IDA Non-Standard Document NS D-8008

A State Cyber Hub Operations Framework

Laura A. Odell, *Project Leader*

Cameron E. DePuy
J. Corbin Fauntleroy
Andrew S. Ferguson
Robert M. Rolfe

FOREWORD

The Department of the Defense, Office of the Chief Information Officer (DoD CIO) is beginning to share knowledge and create templates that the states and territories can leverage nationally. The Institute for Defense Analyses (IDA) assisted the DoD CIO in formalizing a proof of concept for cyber initiatives and developed frameworks for operationalizing the data and intelligence produced across state structures and organizations. The framework presented in this document is the culmination of discussions and decisions regarding state cyber organizations and decision support models collected in a formal workshop convened at IDA on May 19, 2016. Information contained in this document is applicable to any state that is trying to gain a better understanding of the cyber environment within its boundaries.

This study, an abbreviated 45-day "sprint" effort, was undertaken in order to provide an initial look at the formulation of a Cyber Hub Operations Framework and to explore a potential decision support model for use within the framework. While States are pursuing the resolution of cyber issues across many fronts, a significant gap remains between the ability to gather and share information and intelligence and the mitigation of breaches that have already occurred.

We focus our attention on the transition from a compliance-based cybersecurity model—one focused primarily on the state of networks, malware, and patching—to a risk-based cybersecurity model that enables a predictive capability to potentially thwart impending cyber-attacks. Operationalizing the analysis of data, information, and intelligence from disparate sources across multiple service sectors in order to provide a common operating picture for State governments, law enforcement, Emergency Services, Homeland Security, National Guard, industry and international stakeholder "partners," and others must begin now. There are no silver bullets, no standardized processes and procedures, and no effortless results. The opportunity to innovate, test (and fail), learn and build a cyber knowledge base that does not exist today is real. As cyber leaders, we must have the business courage to make decisions that do not "fit" with traditional paths and models for how we conduct business today. Our adversaries will not take a traditional approach to attacking us. We must not take a traditional approach to stopping them.

This document is intended to provide a place to start for State leaders who envision an ability to operationalize intelligence and information in a way that can stay ahead of the curve when it comes to cyberattacks. It is the opening salvo in a large and complex journey and provides some initial thinking to get things started. Action is driven by discussion, decision-making, and resourcing. It was our intent to drive progress in all of these areas as a result of our work.

The Cyber Hub Study Group:

Ms. Betsy L. Freeman, Study Group Chair, DoD CIO
Ms. Laura Odell, IDA
Ms. Cameron DePuy, IDA
Dr. Robert Rolfe, IDA
Dr. Corbin Fauntleroy, IDA
Mr. Andrew Ferguson, IDA
Ms. Edna Jordan, IDA
Mr. Matt Coursey, IDA
Mr. Scott Gannon, IDA
Mr. David L. Phillips Jr., BAH

This page intentionally left blank.

EXECUTIVE SUMMARY

Over the last decade, the cybersecurity landscape has changed dramatically. Cybersecurity concerns are now center stage at all levels of industry, government, and the law enforcement and emergency services communities. While progress has been made in efforts to gather and share intelligence, data, and information, a significant gap remains between the ability to gather and share information and the ability to predict impending cyber-attacks and to thwart them before they are successful. It is with this thought in mind that the Cyber Hub Study Group began its work to create a Cyber Hub Operations Framework. This model is intended to leverage, not replace, existing organizations and structures, and it begins the work toward an operational cyber construct that is risk-based versus compliance-based.

Decision support is the core function of the Cyber Hub's mission. The ability of an organization to operate, organize, anticipate, and respond to an event, from initial situational awareness through restoration and feedback capture, requires a capability that can be undertaken only with the adoption of an operational model based on common processes and standards. It requires, at a minimum, best-of-breed processes, state-of-the-art data grooming, and an agile decision support model.

Decision-making is a recurring cycle of: Observe – Orient – Decide – Act (OODA). The "OODA Loop" is a model for understanding decision-making as an iterative process; a decision is reached through observing an evolving situation, orienting and reorienting based on those observations, developing a response plan based on continuous observation and orientation, and then executing the decided action. The OODA decision model forms the foundation of the Cyber Hub Operations Framework.

Each element of the OODA decision model takes in information from different sources, including data, intelligence, historical scenarios from participating stakeholders, existing data lakes, historical/exercise outcomes, and ongoing and real-time situations for analysis. This information informs the work within each element. The end result of the Cyber Hub Operations Framework is an ever-evolving cyber knowledge base, a state of constant observation, continuous learning via a Cyber Playbook, continuous training scenarios, and a shared common operating picture.

The Cyber Hub cannot become a reality without cooperation and communication across a range of stakeholders (Federal, state, local, industry, academia, international, law enforcement, and others). All stakeholders should be invited to participate in the Cyber Hub, bringing data and expertise in the creation of a fuller cyber operational picture. Stakeholders can become subscribing members to the Hub by agreeing to the framework charter. Membership in the Hub provides: cyber event decision support, access to the common operating picture, the Cyber Playbook, and an ever-expanding cyber event knowledge base and training opportunities.

The way ahead is unique to each state that may decide to implement the Cyber Hub Operations Framework and decision support model as outlined in this study. Each state must take stock of the resources, investments, organizations, structures, and overall progress the state has made to date against its own strategic cybersecurity goals. By combining resources across all members, the Cyber Hub will enable a more secure cyber ecosystem within the state.

This page intentionally left blank.

TABLE OF CONTENTS

This page intentionally left blank.

A STATE CYBER HUB OPERATIONS FRAMEWORK

INTRODUCTION

Over the last decade, the cybersecurity landscape has changed dramatically. Cybersecurity concerns are now center stage for industry boards of directors, state and local governments at all levels, and law enforcement and emergency services communities. While significant progress has been made in efforts to gather and share intelligence, data, and information from numerous sources via industry sector, Federal and state-based fusion centers, and Information Sharing and Analysis Centers (ISACs), a significant gap remains between the ability to gather and share information and the ability to predict impending cyber-attacks and stop them before they are successful. It is with this thought in mind, that the Cyber Hub Study Group began its work to create a Cyber Hub Operations Framework, including a decision support model and an advanced analytic capability, providing a common operating picture across all subscribing members. This model would leverage, not replace, existing organizations and structures and begin the work toward an operational cyber construct that is risk-based versus compliance-based.

Where do you begin?

While the Internet of Things continues to enable a connected world and positively drive global commerce, communication, and cooperation, it has also enabled terrorists, criminals, and other malicious actors to more easily steal, disrupt, and destroy information. Furthermore, technology platforms, given the scope and criticality of the items they control, are bigger targets than ever before. Finally, the proliferation, use, and generation of data continues to grow and has become a tool for terrorists, criminals, and other bad actors to monetize to their advantage. So where do you begin? The answer is, begin wherever you are!

Each state has its own ongoing cyber efforts, unique structures, organizations, and roles and responsibilities. This framework was built with those things in mind, thus it is a framework and not an implementation guide. While this document offers specifics on how operations could be launched, it stops short of making recommendations. It is meant only to launch discussions about the possibilities and offer ideas based on an existing example state structure. The document presents the basic concepts underlying and discussions surrounding the operations, manpower, governance, and resourcing of such an effort. However, state decision makers will determine the appropriate application, structure, and resourcing based on their unique state or regional approach.

Two critical factors in moving forward, from the study group's perspective, are:

- Begin discussions and planning for a Cyber Hub today. Do not get stuck in a discussion–discovery loop and fail to act.
- Address barriers to progress with a sense of urgency and innovation. Focus on ways to succeed rather than on assessing people, processes, and technology.

The Cyber Hub Concept: Focused on Decision Support Outcomes

The State Cyber Hub is an enterprise framework whose core function is decision support to state officials and all other relevant stakeholders. The mission of the Cyber Hub is to operate, organize, anticipate, and respond to an event, from initial situational awareness through restoration and feedback capture. It requires a capability that can be undertaken only with the adoption of an operational model based on common processes and standards. This mission requires, at a minimum, best-of-breed processes, state-of-the-art data grooming, and an agile decision support model. The Cyber Hub Operations Framework enables understanding of an evolving cyber situation resulting from continuous observation across all critical infrastructure sectors.

A shared common operating picture (COP), based on current and predictive analytic capabilities, will encourage collaboration among participating stakeholders—Federal, state, local, law enforcement, industry, National Guard, and international partners—in and around the Cyber Hub. Using a coherent, data-driven methodology, Hub operators can inform, assess, and adapt potential responses to a cyber scenario for local, accountable decision makers, enabling them to act with the broadest information and intelligence available at the time.

Because of the breadth of potential hub-level cyber operations—from state information technology (IT) and network infrastructure to hospitals, commercial banking, and manufacturing—the concepts in the framework focus on mission agility and a broad-based collaboration capability. The framework addresses:

- Employment of existing intelligence capabilities at the Federal, state, and local levels;
- Development, maintenance, and evolution of a COP; and
- Effective command structures that enable self-synchronized[1], agile operations.

Guiding Principles

This effort began with a request from a State Chief Information Officer (CIO) to review progress on the state's formalized cyber initiatives and provide a potential path for operationalizing the data and intelligence produced across various state structures and organizations. The CIO had a singular goal in mind: transition the state from a compliance-based cybersecurity model to a risk-based model while expanding partnerships with industry and government at the international, Federal, state, and local levels. Working within a 45-day timeline, the Cyber Hub Study Group began its effort by developing a set of guiding principles to serve as guideposts for all discussions and analysis. These principles, listed below, served as the departure point in the consideration of any potential changes to existing personnel structures, existing policy, and technology requirements.

[1] The ability for a well-informed organization to organize and synchronize complex activities from the bottom up.

Guiding Principles

- Lead with the "Cyber Hub" concept in order to facilitate stewardship;
- Create an enterprise framework with common technical standards and processes as the default, leveraging existing models;
- Optimize the use of data, information, and intelligence from existing programs (including fusion centers and ISACs), platforms, and tools in order to build and continually strengthen all operational outcomes;
- Define and establish governance to promote transparency and cooperation; and
- Drive mission agility through communication and collaboration.

Methodology

The Cyber Hub Study Group followed a four-phase approach to the research: collaborate, collect, analyze, and inform. The group met with subject matter experts and key stakeholders to produce a pre-decisional working document. To ensure full transparency, the study group contacted as many stakeholders as possible within the limited timeframe of this analysis to collect and gather relevant information.

The group collected and analyzed information from a large body of authoritative data sources, including Federal, state, Department of Defense (DoD), and web-based sources, as well documents in the Institute for Defense Analyses document archives. In all, over two hundred documents and other sources were analyzed. The list of sources used to support the development of this document is contained in Appendix A.

This document is a result of the analysis of source documents and data collected from discussions with subject matter experts and key stakeholders.

Purpose

The Cyber Hub is defined as the operational decision support capability (engine) for cyber operations within the state. Its purpose is to operate, organize, and respond to an event, from initial situational awareness to resolution and capture. Inside the Hub, a "response" constitutes the analytic outputs/products provided through a shared COP dashboard capability. Potential response scenarios are dynamically built from ongoing observations, historic data, and trends. Continuous cyber observation—coupled with shared information, advanced analytics, and Human-in-the-Loop (HITL) experts—will provide decision makers the best available information to prevent incoming or ongoing events and capture information to strengthen the ability to predict and respond in advance of the next scenario.

The success of a Cyber Hub depends on four foundational operational principles: communication, collaboration, cooperation, and collocation. Many existing structures and organizations contain one or more of the above concepts. What makes a Cyber Hub different is its ability to operationalize all concepts together. The ability to operate, organize, and respond to an event from start (e.g., situational awareness) to finish (e.g., restoration) requires best-of-breed processes, state-of-the-art data grooming, and an agile decision support model. The Cyber Hub provides a COP, enabling stakeholders to understand their roles and responsibilities and the state to quickly and effectively act on informed decisions. An example infographic of a COP may be found in

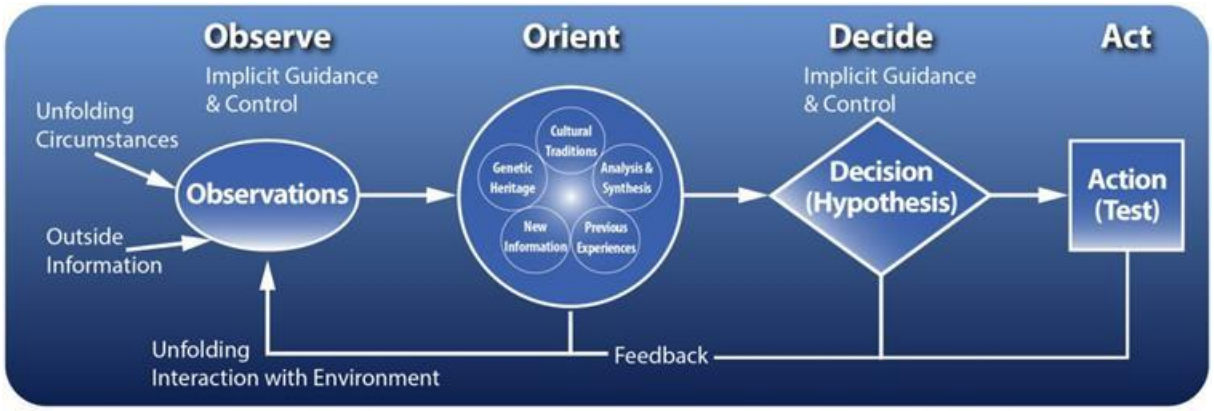
Appendix F. The Cyber Hub is not intended to replace existing organizations or governance structures. Rather, it will leverage the capabilities of the existing structures in order to operationalize decision-making.

Concept of Operations

The foundation of the Cyber Hub is an operational decision-making model that supports situational understanding of a constantly evolving situation. Cyber is a rapidly evolving environment across multiple stakeholders with disparate technologies, making operating in this space challenging and seemingly unstructured.

Decision Support Model – The OODA Loop

Decision-making is a recurring cycle of: Observe – Orient – Decide – Act (OODA). The "OODA Loop," as it has come to be known, is a model for understanding decision-making as an iterative process; a decision is reached through observing an evolving situation, orienting and reorienting based on those observations, developing a response plan based on continuous observation and orientation, and then executing the decided action. Each element of the OODA Loop feeds information forward and provides feedback to the others while embracing and interacting with the environment itself (as shown in Figure 1).



Source: Institute for Defense Analyses, 2016.

Figure 1: OODA Loop Decision Model

The cyclical nature of both the overall process and the iterative interactions among the elements allows the OODA Loop decision model to evolve decisions as situations develop. Cyber events may not be static, so decision-making must not be static either. In each element of the OODA Loop, whose decision processes are discussed below, the HITL processes dominate cyber operations decisions at each stage of response. In some cases, tools that employ machine-learning techniques can take direct action in a network with limited human intervention. Although advanced technologies greatly improve the quality and speed with which we can discover, analyze, and retain data, machine learning alone is never sufficient for final decision-making. When a machine does take automated action, that action is based upon pre-approved courses of action.

The rapidity at which one is able to complete the OODA Loop elements is dependent on learning from the past. The OODA Loop model is a repeatable process that provides for continuous learning and training opportunities. Reaction to each new cyber incident will be informed by previous iterations of processes within the OODA Loop. Capturing a record of the iterations will allow easy reference and documentation to be carried forward and support the pre-planning of standard scenarios.

The Cyber Hub uses the OODA Loop model as the basis for a Concept of Operations (CONOPS). The CONOPS, provided below, depicts the employment of the communication, collaboration, cooperation, and collocation of the Cyber Hub for all elements of the OODA Loop. Although the elements are presented as if they were linear, the various functions are done in parallel as they feed forward and backward. In order to understand how a Cyber Hub could operate, the following sections:

- Describe each of the OODA Loop elements in the context of the Cyber Hub,
- Identify inputs to and outputs of each element, and
- Provide considerations for action within each element.

Observe

The Cyber Hub does not operate only when a cyber event occurs but exists in a constant state of observation. The Observe Element is the process by which intelligence and information products are gathered, data is groomed for content and analytics, and information is shared. When a cyber event occurs, the unfolding circumstances are captured and data from the environment is collected. This element significantly relies on communication and cooperation. Many of the existing organizations within a state will play a role in this element and provide critical inputs to the Cyber Hub. The Cyber Hub does not create new intelligence, but rather leverages existing organizations with those capabilities and missions to recognize significant activities within the environment to the best extent possible given the available resources.

In the Observe Element, the Cyber Hub accepts available intelligence products from all sources. A regular review of alerts and situation reports (SITREPS) will trigger response processes. The initial response processes fall into one of a set of predefined categories (e.g., an attack on a localized and/or statewide infrastructure operator). The response processes will trigger a request for preparation of additional intelligence information based on pre-planning, previous experience, and possibly lessons learned. Further, it is likely to cause the Hub leadership to bring additional expertise into the Hub team from a variety of possible stakeholders.

Additional selection of potential raw intelligence feeds and analytical knowledge products drives the discovery process forward. Raw intelligence feeds, human intelligence, and analytic knowledge product requests will be triggered by the Cyber Hub leadership team after receipt of initial alerts and SITREPS. The new data may be in a mix of structured, semi-structured, and/or unstructured formats.

Initial Cyber Hub team assessment will lead to requests for additional data, incorporation of new team members, and preparation of Cyber Hub infrastructure to support operations. The preparation of the request for additional relevant structured and unstructured/semi-structured

information should go through a validation process to ensure the best possible approach has been taken. In addition, warning advice[2] will have to be prepared for potential team leaders and/or identified leadership. Warning advice is composed of one or more basic elements: Situation, Mission, Execution, Service Support, and Command and Signal. These elements provide a description of the operational situation and courses of action that should be taken.

As part of the Cyber Hub's liaison responsibilities early on in a situation, an adaptive process of data grooming needs to take place. The basic steps in data grooming include:

- Metadata tag incoming and/or available information:
  - Requires tools and a knowledge base to support the Cyber Hub processes.
- Extract content state and object information:
  - Apply supervised and unsupervised machine learning algorithms to assist in tagging data by context and content to separate related information into topic group clusters and collect data in a query-able knowledge base.
  - Use Natural Language Processing (NLP) tools for the capture and extraction of structured information concerning spatial and temporal relationships for objects, actors, events, and activities, enabling the creation of knowledge supporting situational understanding.
  - Provide initial visualization of spatial, temporal, and other contextual relationships for objects, actors, events, and activities (includes implicit and explicit known relationships between entities). Visual backdrops might be geospatial, but might also show results against an enumerated set, e.g., affected sectors of the communication system, the power system, the water and sewage system, or any other enumerated set of objects.
  - Identify entities and filtering attributes, such as political, military, cultural, civic, social, environment, economic.
  - Determine existing and potential knowledge gaps by querying available event data.
  - Identify potential sources of data and additional information needed to fill the knowledge gaps.

Certain information derived from intelligence sources, methods, or analytical processes are legally required to be handled within formal control systems to ensure the information's protection and integrity. This information is known as Sensitive Compartmented Information (SCI). The Cyber Hub will need to follow the established formal control systems for the handling, processing, discussion, and safe storage of SCI to protect against unauthorized or unlawful disclosure. A full discussion of SCI can found in Appendix C.

Observe – Inputs and Outputs

During the Observe Element of the OODA Loop, several information sources and tools are used by the Cyber Hub to collect data and understand the environment. These sources and tools include:

[2] A preliminary notice of an order or action which is to follow. This initiates the development and evaluation of courses of action by a commander outside the Hub and requests that a commander's estimate of response be provided.

- Alerts, SITREPS, and immediate assessments of the situation from affected organizations.
- Feeds from cyber defense relevant systems, including: Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), social media, live network feeds, law enforcement agencies (LEA), ESRI, intelligence, firewall functions, Remedy, Palo Alto, Spectrum, NetFlow, ArcSight, BlueCoat Proxy, management control systems, enterprise management functions, routing/switching functions, Tor,[3] Black List actors, publically available sources on Internet service providers, and Department of Energy Visualizing Energy Resources Dynamically on Earth (VERDE) Critical Infrastructure Program.
- Pre-planned scenarios and training exercises, previous OODA iterations, and captured, query-capable knowledge base, which are organized into a Cyber Playbook. These items are codified in terms of tactics, techniques, and procedures formulated previously to support the response process, hence the name playbook. The playbook templates are situationally dependent and include the decision history and results captured in a knowledge base, which can be used to replay and understand what happened. The templates are pre-prepared checklists to help the Cyber Hub team walk through the process steps for all elements of the Cyber Hub OODA Loop.[4]

The Observe Element produces shared outputs from the Cyber Hub. These include:

- Actionable intelligence – Initial information sharing through the COP and shared knowledge base, all distributed in a number of formats depending on the infrastructure available to the stakeholders.
- Preliminary feedback – Warning, operation advice, and fragmentary updates as needed.[5]
- Operational advice – Which has five basic elements, including: Situation, Mission, Execution, Service Support, and Command and Signal.[6]

Orient

Orientation represents images, views, or impressions of the situation shaped by previous experiences, and unfolding circumstances.[7] Orientation is an interactive process involving cross-reference of projections, empathies, correlations, and rejections that shape the way we perceive, decide, and ultimately act on observations. While the Observe Element receives information and data, the Orient Element provides context and understanding to that information. Within the Orient Element, the Cyber Hub and its stakeholders, collocated physically or virtually, can structure the decision-making process with context knowledge and previous experience.

The core mission of the Orient Element is to provide previously acquired knowledge to newly observed events. Through marrying observations with situational awareness and subject matter expertise, the Cyber Hub will be able to properly orient itself toward meeting the challenges of

[3] A free software implementation of second-generation onion routing, a system enabling its users to communicate anonymously on the Internet.

[4] The technology and infrastructure to support the playbook involves basic IT services for document creation, management, and distribution and should be built around a knowledge base that can be queried with a standard library of queries.

[5] https://en.wikipedia.org/wiki/Five_paragraph_order

[6] http://www.policemag.com/channel/patrol/articles/2012/01/operations-plans.aspx

[7] OODA descriptions emphasize genetic heritage and cultural tradition, which may be less of a factor in some cyber events.

any event. In order to collect the observations and put them into a relevant context, the Cyber Hub must:

- Categorize cyber event situation by primary impact areas;
- Identify prior relevant knowledge by using Cyber Hub on-line resources and external resources;
- Identify previous mitigation and recovery approaches (e.g., tactics, techniques, and procedures that might be effective) using team, knowledge base, and external resources;
- Continue to update the COP and provide to relevant external collaborators;
- Estimate cyber actors' intent and capabilities in coordination with other observations;
- Identify patterns of behavior often unique to specific cyber actors and teams and countries of origin, which are not necessarily those of attribution;
- Organize observations into a working hypothesis of the situation and possible consequences;
- Identify knowledge gaps and issue requests for additional information team participation as needed;
- Formulate a proposed response plan and alternatives using team knowledge in conjunction with available decision-support resources, systems, and tools; and
- Identify risks introduced in association with a proposed planning response.

Orient – Inputs and Outputs

During this element of the OODA Loop, inputs from observations are correlated with inputs from previous experience, situational awareness, and subject matter expertise.

- Inputs are continual integration of incremental updates from all sources.
- Outputs include information sharing updates through the COP and shared knowledge base—all distributed in a number of formats depending on the infrastructure available to external team members.
- Additional outputs include preliminary warning advice, draft operation, and possible fragmentary updates as needed.

Decide

The decide element of the OODA Loop is the determination of a course of action (COA) based on the current mental perspective of the Cyber Hub team. The COA is developed according to a hypothesis of the current situation and approaches to mitigate it. This includes selecting the appropriate team members (subject matter experts and mitigation actors) to formulate COAs, conduct risk assessments, and design response approaches. Additionally, the Hub operators will communicate with and collaborate on the development of COAs with relevant stakeholders and act according to statutory and agreed-upon state policy and governance procedures when completing the Decide Element of the OODA Loop. It is essential to know that in the background, knowledge gaps are continually being identified in order to provide near-real-time output for the decision maker.

In order to develop a plan of action, the Cyber Hub must:

- Identify a Cyber Hub response team, including Cyber Hub Battle Captain, on-site members, and external response team members and partners;
- Assess Cyber Hub team status though mission readiness status checklist;
- Develop a hypothesis of the current situation and approaches to mitigate it;
- Develop proposed COAs based upon a consensus of the Cyber Hub team;
- Identify remaining and continuing knowledge gaps;
- Identify alternative mitigation approaches;
- Identify potential risks related to all mitigation approaches;
- Consider second- and third-order effects and consequences for all potential mitigation approaches;
- Re-evaluate response alternatives, prepare outline of the COA, and conduct final review of resource status and planning and draft orders as required;
- Formulate a COA;
- Prepare final planning and advice;
- Prepare strategic information operations material;
- Advise and coordinate COAs and expectations with state leadership; and
- Seek advice and consensus with external team members.

Decide – Inputs and Outputs

During the Decision process, inputs from all elements are correlated and streamlined to inform a comprehensive and actionable decision. This decision will have the following:

- Input: Continuous integration of incremental updates from all sources and
- Output: Updated common operating picture and intended COA advice.

Act

In the Act Element of the loop, Hub operators implement, monitor, and capture the response plan. This element is seen as the "last call" for the operators because they must now capture the outcome of unfolding events following the final choices of the decision maker. This includes providing agile and coherent response operations formulated by the Cyber Hub incident response team. Observation continues, including risk assessment and reporting cyber alerts and network operations impacts and anomalies. In this element, the Hub operators will update the Cyber Playbook, enabling current and future decision support. Finally, the Hub operations team must track and report key performance indictors (KPIs) (established by the state) in order to drive ongoing operations monitoring and continuous process improvement. If the state model is extended to a region (e.g., a FEMA Region); then mutually agreed-upon core KPIs should be identified and reported at this time.

The goal of the Act Element is to implement the decision made as a result of the OODA Loop Process. In order to fully enact the decision, the Cyber Hub must do the following:

- Implement the response plan;
- Finalize risks related to the response;

- Consider alternatives;
- Formulate COAs for implementation;
- Prepare execution advice with the finalized response team selection;
- Gain approval from relevant authorities;
- Finalize public affairs announcements and information operations;
- Release advice and monitor implementations; and
- Execute the correct response plan as required.

Act – Inputs and Outputs

In order to Act effectively, continuous input of information from the decision and other elements of the OODA Loop must inform output actions. For the Cyber Hub, these inputs and outputs include:

- Inputs:
  - Continuing intelligence and monitoring of inputs;
- Outputs:
  - Configurable visualizations of near-real-time data providing a detailed representation of: cyber readiness (risk assessment), cyber alerts, and network operations;
  - Agile and coherent response operations formulated by the Cyber Hub incident response team;
  - Predictive cyber response effects and recovery;
  - Dynamic and adaptive playbook updates for current and future decision support;
  - Cyber event capture trend analysis and forensics; and
  - Anticipated key performance indicators to drive ongoing operations, monitoring, and continuous process improvement.

Critical Planning and Success Factors

The Cyber Hub Operations Framework implementation has a number of critical planning and success factors for operations, governance, manpower, and resources, listed below. These factors can be implemented in planning cycles with the necessary investment and other resources.

Operations

- Develop methods for observation, including:
  - Gaining access to all relevant networks in the cyber operations hub and in the associated Sensitive Compartmented Information Facilities (SCIFs) (described in Appendix B), and
  - Obtaining IT infrastructure and tools required for data grooming, including intelligence search algorithms.
- Create playbook content including:
  - Developing pre-planned event templates, which will continue to evolve over time; and

  - Archiving CONOPS and experiences captured at many levels, from a preplanned operational checklist for the commander to specialized products and services and how and to whom they are to be distributed.

- Test and validate all forms of communication and collaboration on a regular schedule. Maintain a database of communication point of contacts (POCs) and test regularly.

Manpower

- Provide training for communications and collaboration support infrastructure.
- Obtain necessary security clearances for Cyber Hub operations teams, including potential surge members and those members of the team who may operate within the Hub and an associated SCIF.
- Develop training plans, programs, and staff to ensure that Cyber Hub operations are ready to operate whenever needed, to include conducting:
  - Individual training (e.g., the Merit Networks Cyber training),
  - Exercise training from a HITL Cyber Incident Model Evaluation Test Bed, and
  - Research and development for training to create new intelligence training capabilities.
- Create an infrastructure support and development team for the Cyber Hub.

Governance

- Develop a plan to modify state and local legislation that might limit communication and collaboration, or create legislation that would improve communication and collaboration.
- Develop memoranda of understanding (MOUs) between stakeholders as required—to be maintained as a portfolio.
- Develop a risk mitigation plan to minimize the impacts on data collection, communications, and collaboration.
- Establish a cyber management framework for decision-making.
- Define an enterprise architecture for the cyber ecosystem.

Resources

- Identify, develop, and maintain the infrastructure needed to support communication and collaboration.
- Provide configuration management for necessary infrastructure.
- Create a core team for the OODA Observe Element, with the roles and responsibilities discussed previously.
- Obtain space adequate for the normal and surge teams within the Cyber Hub, with ingress and egress resource areas, and able to sustain human function across multiple-day operations.
- Identify the necessary investments and personnel, including:
  - Multi-year and current year budget planning;
  - Organizations, including industrial base, government, not-for-profits, academia;
  - Funding, memoranda of agreement (MOAs), standing relations, events, and exercises;
  - Communications and IT infrastructure alternatives;
  - Line-of-site (LOS) radio and satellite networks;

- Power network; and
- Integration of commercial-off-the-shelf (COTS), and possibly government-off-the-shelf (GOTS), computer tools needed to increase operating efficiency of Cyber Hub team.

THE WAY AHEAD

The Way Ahead is unique to each state that may decide to implement the Cyber Hub Operations Framework and decision support model as outlined in this document. Each state must take stock of the resources, investments, organizations, structures, and overall progress it has made to date against its own strategic cybersecurity goals. This "as is" picture is the place from which to begin discussions on a potential Cyber Hub capability within the state. Offered here for your consideration are some concepts that appear to be applicable to all states.

Facts + Realistic Timelines + Resources = Success

The key ingredient to successful action is fact-based research, realistic implementation timelines, and identifying resources and leadership action. While many efforts look to achieve an 80% solution and complete stakeholder agreement to start, it is the experience of this study group that those parameters, while very risk-sensitive, may stifle innovation, extend timelines for implementation, and give way to the bureaucratic processes that are barriers to progress.

Goods News and Bad News

The good news is that work in the cyber domain is in its infancy, so there is significant opportunity for innovation. Additionally, there are many ongoing efforts across the country. So before you begin, talk with others who may have already begun the journey. Partner, wherever possible, with ongoing efforts, because it will likely save precious time and resources. The bad news is that the cyber domain is in its infancy and a lack of processes, technology, and a ready cyber workforce can easily become barriers to progress. The Way Ahead is a call to action!

Next Steps

The Cyber Hub Operations Framework is dependent on four key pillars—Operations, Manpower, Governance, and Resources. Senior Leader decisions must be made and actions taken that will be critical to the timely delivery of a functional, agile Cyber Hub. Consider these next steps, for each of the four pillars, as you continue on your cybersecurity journey.

Operations

The Cyber Hub is envisioned to be operating 24/7 and will require operating procedures that allow stakeholder participation. This starts with the implementation of the OODA decision model and fleshing out the processes and procedures for observing, orienting, deciding, and acting. It continues with the development of the Cyber Playbook, which contains preliminary scenarios that will be continuously updated with responses across all sectors. Any SCIF mission requirements should be identified and clearance reciprocity processes developed. All forms of communication and collaboration that occur on a regular schedule should be tested and validated.

Manpower

Having people with the right skill sets is important for successful implementation. States should establish and identify the Cyber Operations Officer who will have responsibility for the overall management of the Cyber Hub. A skill gap analysis should be conducted against the Cyber Hub operational roles and responsibilities to identify deficiencies in the workforce. Any limiting factors with State Government/National Guard hiring practices should be identified. Waivers may need to be employed to obtain qualified personnel. Potential legislation changes may be necessary to sustain a capable cyber workforce over time.

Existing and new personnel will require specific training. It is important to identify hub training requirements based on skill sets and sources, both in-residence and distance learning, to meet qualification needs. In addition, it may be necessary for Cyber Hub team members to obtain and maintain clearances for SCIF access.

Governance

Governance, which establishes leadership mechanisms, is a crucial element of meeting Cyber Hub objectives. An overarching governance strategy and implementation plan provides the foundation for an organizational construct empowered as the approval and directive authority for all cyber and information technology for the State CIO, with operational feedback from stakeholders (see Appendix C). Key stakeholders can prioritize critical infrastructure cyber issues within this framework.

A Charter agreement and memoranda of understanding can clearly establish the organizational construct and define oversight roles and responsibilities for subscribing members and stakeholders. Because structures across each state vary and authorities may not be aligned, an additional decision point for consideration, based on a State's legislation, is whether or not the sample Cyber Hub Management Construct charter (see Appendix D) can be modified for adoption. The ideal construct is centralizing decision-making at the state level to achieve the synergy required among stakeholders.

Resources

A State Cyber Hub will require additional resources in terms of funding and infrastructure. States will need to identify their financial requirements and correlate them to funding sources (Federal, state, and local) across the initial operation capability–final operating capability timeline. Other cybersecurity facilities across the state may need to provide information and data to the Cyber Hub. Relationships should be developed with facility stakeholders to capture critical information that will feed the COP. Key cyber team members should be collocated to the Cyber Hub as soon as possible. Government employee space requirements should be determined to facilitate optimal collaboration through co-location. Finally, the information technology infrastructure requirements should be validated to enable collaboration and dashboard capabilities.

CONCLUSION

This study was prepared as a "sprint" effort to further energize discussions across state government and industry on the possibilities of how to operationalize shared cyber data and

intelligence to our best advantage. The examples and ideas presented in this paper are viewed as a place to start when exploring some of the associated complex and thorny issues.

It is the hope of the Cyber Hub Study Group that this work will drive frank and open discussions on how to begin moving from a compliance-based cybersecurity model to a risk-based cybersecurity model. The study provides samples and examples of concepts that could be applied across various existing structures and organizations. Appendix E provides a graphical representation of many of the concepts in this document that can be used as a starting point for discussion. This document is intended to be a further call to action to all leaders who work in this emerging cyber domain. The strength of execution will be evidenced in the ability to collaborate, communicate, cooperate, and co-locate. That will take business courage and the fortitude by leaders at all levels when the going gets tough. Our cyber adversaries cannot out-flank us. Failure is not an option. For this reason, we encourage leaders to read this study and use it as a launch pad for moving to the next level of maturity on your cyber efforts no matter where you are today.

Ultimately, current progress and cooperation on cybersecurity issues at the Federal, state, and local levels is unprecedented. Every service sector in industry has also become a critical element of the partnerships that will create cyber solutions. We need all stakeholders at the table to share information and have robust discussions. We do not always have to agree on issues and we will not. What is important is that we find a way to address the new challenges of this cyber domain together.

We will only succeed if we can have the tough discussions, make decisions, eliminate barriers, and act.

Let’s go!

APPENDIX A: BIBLIOGRAPHY

Adamo Construction. (2016). *SCIF Glossary of Terms*. Retrieved from http://www.adamoconstruction.com/scif-glossary.php

Air National Guard. (2015). *Fiscal Year (FY) 2016 Budget Estimates: Military Construction Justification Data Submitted to Congress*. (Appropriation 3830). Washington, DC.

Air National Guard. (2015). *Selfridge Air National Guard Base: Tomorrow's Military Installation Model Today*. Retrieved from http://www.127wg.ang.af.mil/shared/media/document/AFD-120919-017.pdf

American Society of Civil Engineers Michigan. (2009). *Michigan Infrastructure Report Card: Not Making the Grade*. Lansing, MI.

Army National Guard. (2015) *Annual Financial Report FY 2015*. Washington, DC.

Boston Joint Terrorism Task Force. (2006). *Memorandum of Understanding between Boston PD and the FBI to combat terrorism.* Boston, MA.

Budde, Brian. (2015, August 3). *Privacy Policy for the MIOC* (Memorandum UD-040). Lansing, MI.

Chief National Guard Bureau (2015, November 16). *National Guard Access to Top Secret Sensitive Compartmented Information* (CNGB Instruction 2200.01). Washington, DC.

Christensen, P. (2015). *Cybersecurity T&E and National Cyber Range*. Presentation prepared for US Digital Service. Washington, DC.

Cofer, R. (2014). *Physical Security of Sensitive Compartmented Information Facilities* (Presentation). Naval Facilities Engineering Command. NAVFAC Atlantic. Washington, DC.

Committee on National Security Systems. (2010, April 26). *National Information Assurance (IA) Glossary* (CNSS Instruction No. 4099). Washington, DC.

DARPA. (2008). *The National Cyber Range: A National Testbed for Critical Security Research.* Arlington, VA.

Denman, T. (2015, February 4). *Cybersecurity and the Risk Management Framework for DoD Information Technology*. Defense Acquisition University Presentation. Huntsville, AL.

Department of Defense. (2014, March 14). *Cybersecurity* (DoD Instruction 8500.01). Washington, DC.

Department of Defense. (2015). *Voluntary Education Partnership Memorandum of Understanding*. Washington, DC.

Department of Defense. (2015, July 1). *Cybersecurity Test and Evaluation Guidebook* (Version 1.0). Washington, DC.

Department of Defense (2013, August 29). *Law Enforcement Defense Data Exchange* (D0D Instruction 5525.16). Washington, DC.

Department of Defense. (2012, October 19). *Sensitive Compartmented information (SCI) Administrative Security Manual: Administration of Information and Information Systems Security* (DoD Manual 5105.21 Volume 1). Washington, DC.

Department of Defense. (2012, October 19). *Sensitive Compartmented information (SCI) Administrative Security Manual: Administration of Physical Security, Visitor Control, and Technical Security* (DoD Manual 5105.21 Volume 2). Washington, DC.

Department of Defense. (2012, October 19). *Sensitive Compartmented information (SCI) Administrative Security Manual: Administration of Personnel Security, Industrial Security, and Special Activities* (DoD Manual 5105.21 Volume 3). Washington, DC.

Department of Defense (2013, October 1). *Sensitive Compartment Information Facilities Planning, Design, and Construction* (Unified Facilities Criteria 4-010-05). Washington, DC.

Department of Defense (2015, July 8). *DoD Facilities Pricing Guide* (Unified Facilities Criteria 3-701-01). Washington, DC.

Department of Defense (2015, September). *Multi-service Tactics, Techniques, and procedures for Defense Support of Civil Authorities*. (ATP 3-28.1; MCWP 3-36.2; NTTP 3-57.2; AFTTP 3-2.67). Washington, DC.

Department of Defense (1985, July 11). *Memorandum of Understanding between DOJ and DOD relating to the Investigation and Prosecution of Certain Crimes* (Memorandum 18-2). Washington, DC.

Department of Defense. (1994, April 20). *Memorandum of Understanding between Departments of Defense and Justice on Operations other than War and Law Enforcement*. Washington, DC.

Department of Homeland Security. (2009). *Civil Liberties Impact Assessment for the State, Local and Regional Fusion Center Initiative*. Washington, DC.

Department of Homeland Security. (2010). *Tribal Participation in Fusion Centers.* Washington, DC.

Department of Homeland Security. (2012). *The Role of Fusion Centers in Countering Violent Extremism.* Washington, DC.

Department of Homeland Security. (2010). *Privacy, Civil Rights, and Civil Liberties Compliance Verification for the Intelligence Enterprise.* Washington, DC.

Department of Homeland Security. (2004, September 17). *Sensitive Compartmented Information Program Management* (DHS Management Directive 11043). Washington, DC.

Department of Homeland Security. (2015, January 16). *Safeguarding Personal Information Collected from Signals Intelligence Activities* (DHS Policy Instruction IA-1002). Washington, DC.

Department of Homeland Security (2013). *DHS Information Sharing and Safeguarding Strategy*. Washington, DC.

Department of Homeland Security. (2011). *Health Security: Public Health and Medical Integration for Fusion Centers*. Washington, DC.

Department of Homeland Security. (2008). *Baseline Capabilities for State and Major Urban Area Fusion Centers: Supplement to the Fusion Center Guidelines.* Washington, DC.

Department of Homeland Security. (2016). *DHS State and Local Law Enforcement Resource Catalog* (Volume IV). Washington, DC.

Department of Homeland Security. (2009). *Law Enforcement Cyber Incident Reporting.* Washington, DC.

Department of Homeland Security. (2011). *Enabling Distributed Security in Cyberspace: Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Action*. Washington, DC.

Department of Homeland Security. (2008). *Memorandum of Understanding among the Department of Homeland Security, the Department of Justice Federal Bureau of Investigation Criminal Justice Information Services Division, and the Department of State Bureau of Consular Affairs for Improved Information Sharing Services*. Washington, DC.

Department of Homeland Security. (2010). *Memorandum of Agreement between the Department of Homeland Security and Department of Defense Regarding Cybersecurity*. Washington, DC.

Department of Homeland Security. (2010). *Memorandum of Agreement between US Department of Homeland Security Immigration and Customs Enforcement and New York State Division of Criminal Justice Services.* Washington, DC.

Department of Justice. (2010). *9 elements of an Information Quality Program*. Washington, DC.

Department of Justice (2012). *Privacy, Civil Rights, and Civil Liberties Policy Development Guide for State, Local, and Tribal Justice Entities*. Washington, DC.

Department of Justice (2012). *Privacy, Civil Rights, and Civil Liberties Policy Development Template for State, Local, and Tribal Justice Entities*. Washington, DC.

Department of Justice. (2016). *Cybercrime Training for Law Enforcement: Equipping Law Enforcement with Tools to Investigate Cybercrime.* Washington, DC.

Department of Justice. (2011). *Global Privacy Resources*. Washington, DC.

Department of Justice. (2010). *Federated Identity and Privilege Management Operational Policies and Procedures Guidelines* (Version 1). Washington, DC.

Department of Justice. (2014). *DHS/ DOJ Fusion Process Technical Assistance Program and Services.* Washington, DC.

Department of Justice. (2009). *Fusion Center Technology Resources Road Map: Elements of an Enterprise Architecture for State and Major Urban Area Fusion Centers*. Washington, DC.

Department of Justice. (2006). *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era.* Washington, DC.

Department of Justice. (2010). *Fire Service Integration for Fusion Centers*. Washington, DC.

Department of Justice. (2014). *Technical Assistance Program and Services.* Washington, DC.

Department of Justice. (2008). *Critical Infrastructure and Key Resources: Protection Capabilities for Fusion Centers*. Washington, DC.

Department of Justice. (2012). *Criminal Intelligence Resources Guide: A Collection of Intelligence Information Sharing Products and Resources*. Washington, DC.

Department of Justice. (2010). *Common Competencies for State, Local, and Tribal Intelligence Analysts.* Washington, DC.

Department of Justice. (2010). *FBI Information Sharing and Safeguarding Report 2010.* Washington, DC.

Department of Justice. (2012). *FBI Information Sharing and Safeguarding Report 2012.* Washington, DC.

Department of the Air Force. (2015, November 13). *Criminal Investigations and CI* (AF Policy Directive 71-1). Washington, DC.

Department of the Air Force. (1998, May 1). *Planning Formats and Guidance* (AF Manual 10-401, Volume 2). Washington, DC.

Deputy Assistant Secretary of Defense for Developmental Test and Evaluation. (2016). *National Cyber Range*. Department of Defense. Washington, DC.

Director of Central Intelligence. (2002). *Physical Security Standards for Sensitive Compartmented Information Facilities* (CIA Directive 6/9). Washington, DC.

Director of Central Intelligence. (1994). *Physical Security Standards for SCIFs* (CIA Directive 1/21). Washington, DC.

Director, Operational Test and Evaluation. (2015). *FY 2014 Annual Report*. Department of Defense. Washington, DC.

Executive Office of the President. (2007). *National Strategy For Information Sharing: Successes and Challenges in Improving Terrorism-Related Information Sharing*. Washington, DC.

Executive Office of the President. (2012). *National Strategy for Information Sharing and Safeguarding*. Washington, DC.

Executive Office of the President. (2013). *Government-wide Tracking of Resources for Cyber Activities* (Budget Data Request No 13-34). Washington, DC.

Executive Office of the President. (2015). *Government-wide Tracking of Resources for Cyber Activities* (Budget Data Request No. 15-29). Washington, DC.

Exec. Order No. 12333, 3 C.F.R. (1981).

Exec. Order No. 13636, 3 C.F.R. (2013).

Federal Bureau of Investigation. (2015). *The FBI: Protecting the Homeland in the 21st Century*. Washington, DC.

Federal Bureau of Investigation. (2015). *Cyber Task Forces: Building alliances to improve the nation's cybersecurity*. Washington, DC.

Federal Bureau of Investigation. (2009). *Six Department of FBI Comity Agreements and Memoranda of Understanding*. Retrieved from https://www.governmentattic.org

Federal Bureau of Investigation. (2009). *FBI Plans to Expand Guardian Portal*. Retrieved from https://privacysos.org/blog/fbi-plans-to-expand-guardian-system-to-include-top-secret-information-link-up-with-sentinel-system/

Federal Bureau of Investigation. (2007). *Memorandum of Understanding between the Federal Bureau of Investigation and the Houston Police Department.* Houston, TX.

Federal Laboratory Consortium. (2016). *Technology Transfer Playbook*. Retrieved from https://www.federallabs.org/T2-Playbook

FEMA. (2010). *Considerations for Fusion Center and Emergency Operations Center Coordination: Comprehensive Preparedness Guide*. Washington, DC.

Finklea, K. & Theohary, C. (2015). *Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement*. Congressional Research Service

ForcePoint. (2016). *Arizona Financial Crimes Task Force: A Sureview analytics solution.* Washington, DC. Raytheon.

ForcePoint. (2016). *Law Enforcement: Providing a Highly Secure and Efficient System that Supports an Agency's Mission While also reducing infrastructure costs.* Washington, DC. Raytheon.

Government Accountability Office. (2007). *Federal Efforts are helping to alleviate some challenges encountered by State and Local Information Fusion Centers* (GAO-08-35). Washington, DC.

Information Sharing After September 11: Perspectives on the Future: Hearing before the Select Committee on Homeland Security House of Representatives, 108th Congress (Serial No. 108-52). (2004).

Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108-458, 118 Stat. 3638, codified as amended at 50 U.S.C. § 401 et seq.

Interagency Working Group on Digital Data. (2009). *Harnessing the Power of Digital Data for Science and Society: Report to the National Science and Technology Council*. Washington, DC.

International Association of Chiefs of Police. (2010). *Developing a Cybervetting Strategy for Law Enforcement Special Report*. Alexandria, VA.

International Telecommunications Union. (2012). *Understanding Cybercrime: Phenomena, Challenges, and Legal response.* Geneva, SWITZ.

Lockheed Martin. (2012). *National Cyber Range Flexible Automated Cyber Test Range*. Washington, DC.

Lockheed Martin. (2014). *National Cyber Range Overview*. Department of Defense, Test Resource Management Center. Washington, DC.

Massachusetts Emergency Management Agency. (2014). *After Action Report for the Response to the 2013 Boston Marathon Bombings*. Boston, MA.

Matthews, W. (2015). Building a Cyber Workforce. NGAUS. Retrieved from http://ngaus.org/newsroom/news/building-cyber-force

Merit. (2015). *Michigan Cyber Range*. Map. VSA.

MI Department of Labor and Economic Growth. (2006). *Memorandum of Understanding between MI Department of Labor and Economic Growth, Michigan Commission for the Blind, Michigan Rehabilitation Services, and Central Michigan University*. Lansing, MI.

MI Department of Technology, Management, and Budget. (2015). *Cyber Disruption Response Plan*. Lansing, MI. Executive Office of the Governor.

MI Department of Technology, Management, and Budget. (2013). *Michigan Cyber Disruption Response Strategy: Protecting Michigan's Critical Infrastructure and Systems.* Lansing, MI. Executive Office of the Governor.

MI Exec. Order No. 2012-5. *Establishing the Michigan Intelligence Operations Center for Homeland Security*. (2012). MI Executive Office of the Governor.

MI Exec. Order No. 2016-5. *Creation of the 21st century Infrastructure Commission*. (2016). MI Executive Office of the Governor.

MI Exec. Reorganization Order no. 2009-39. (2009).

MI Executive Office of the Governor. (2015). *Michigan Cyber Initiative 2015*. Lansing, MI.

MI Executive Office of the Governor. (2015) *Department of Defense chooses Battle Creek Air National Guard Base for new Cyber Operations Squadron* [Press Release]. Retrieved from http://www.michigan.gov/snyder/0,4668,7-277-57577_57657-370904--,00.html

MI Executive Office of the Governor. (2012). *Governor launches cutting-edge cybersecurity training program* [Press Release]. Retrieved from http://www.michigan.gov/snyder/0,4668,7-277-57577-289758--,00.html

MI Executive Office of the Governor. (2013). *Governor Snyder working to combat cybersecurity challenges* [Press Release]. Retrieved from http://www.michigan.gov/snyder/0,4668,7-277-57577_60279-313367--,00.html

MI Executive Office of the Governor. (2014). *Michigan and Israel sign industrial R&D collaboration agreement* [Press Release]. Retrieved from http://www.michigan.gov/snyder/0,4668,7-277-57577-330907--,00.html

MI Executive Office of the Governor. (2011). *Michigan Announces Cyber Initiative* [Press Release]. Retrieved from http://www.michigan.gov/snyder/0,4668,7-277-57577_57657-263758--,00.html

MI Executive Office of the Governor. (2014). *Michigan Cyber Range Hub launched at 110th Airlift Wing ribbon-cutting ceremony* [Press Release]. Retrieved from http://www.michigan.gov/snyder/0,4668,7-277-57577_57657-324626--rss,00.html

MI Executive Office of the Governor. (2015). *October 2015: Cyber Security Awareness Month* [Press Release]. Retrieved from http://www.michigan.gov/snyder/0,4668,7-277-57577_59874_72854-366152--,00.html

MI InfraGard. (2016). Michigan Members Alliance Home. Retrieved from https://www.infragard.org/

MI Intelligence Operations Center. (n.d.). Retrieved April 11, 2016, from http://www.michigan.gov/mioc/

MI National Guard. (2015, August 5). *Air National Guard State of the State*. Lansing, MI.

Mussing, E, & Lamb, C. (2011). *Joint Interagency Task Force-South: The Best Known, Least Understood Interagency Success*. Institute for National Strategic Studies Strategic Perspectives, No. 5. Washington, DC. National Defense University Press.

NASCIO. (2014). *2014-2016 Strategic Plan*. Washington, DC.

National Counterintelligence and Security Center. (2015, September 10). *Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities* (Version 1.3). Office of the Director of National Intelligence. Washington, DC.

National Guard Association. (2010). *NGAUS Fact Sheet: Understanding the Guard's Duty Status*. Washington, DC.

National Guard Association. (2015). *Legislative Objectives for Preparation of Fiscal Year 2016 Defense Budget*. Washington, DC.

National Governors Association. (2010). *A Governor's Guide to Homeland Security*. NGA Center for Best Practices. Washington, DC.

National Fusion Center Association. (2014). *National Strategy for the National Network of Fusion Centers*. Washington, DC.

National Science and Technology Council. (2016). *Federal Cybersecurity Research and Development Strategic Plan*. Executive Office of the President. Washington, DC.

National Transportation Safety Board. (2008). *Memorandum of Understanding between the National Transportation Safety Board and the United States Coast Guard Regarding Marine Casualty Investigations*. Washington, DC.

NY Executive Office of the Governor. (2014). *New York State Homeland Security Strategy*. Albany, NY.

NITRD. (2014). *Report on Implementing the Federal Cybersecurity Research and Development Strategy.* National Science and Technology Council. Washington, DC.

NITRD. (2015). *The Networking and Information Technology Research and Development Program: Supplement to the President's Budget*. National Science and Technology Council. Washington, DC.

NITRD. (2010). *Cybersecurity Game-change Research and Development Recommendations*. National Science and Technology Council. Washington, DC.

Norton. (2012). *Law Enforcement and Cybersecurity Cybercrime Report.* Washington, DC.

Nuclear Regulatory Commission. (1991). *Memorandum of Understanding with the FBI* (SECY-99-257). Washington, DC.

O'Brian, R.P. (2012, March 8). *Notice of Response to FOIA Request* (File No. 12-0617). Department of Police of the City of Chicago. Chicago, IL.

Office of Personnel Management. (2015). *Investigations Reimbursable Billing Rates Effective October 1, 2015* (Federal Investigations Notice No 16-01). Washington, DC.

Office of the Director of National Intelligence. (2010, September 17). *Physical and Technical Security Standards for Sensitive Compartmented Information Facilities* (IC Standard 705.1). Washington, DC.

Office of the Director of National Intelligence. (2015, July 24). *Intelligence Community Civilian Joint Duty Program Implementation Guidance* (IC Policy Guidance 660.1). Washington, DC.

Office of the Director of National Intelligence. (2013, June 21). *Protection of Classified National Intelligence, Including SCI* (IC Directive 703). Washington, DC.

Office of the Director of National Intelligence. (2009, June 10). *Reciprocity for Intelligence Community Employee Mobility* (IC Policy Guidance 709). Washington, DC.

Office of the Director of National Intelligence. (2008, October 2). *Personnel Security Investigative Standards and Procedures Governing Eligibility for Access to SCI and other Controlled Access Program Information* (IC Policy Guidance 704.1). Washington, DC.

Office of the Director of National Intelligence. (2008, October 2). *Personnel Security Adjudicative Guidelines for Determining Eligibility for Access to Sensitive Compartmented Information and other Controlled Access Program Information* (IC Policy Guidance 704.2). Washington, DC.

Office of the Director of National Intelligence. (2008, October 2). *Denial or Revocation of Access to Sensitive Compartmented Information, other controlled Access program Information and Appeals Processes* (IC Policy Guidance 704.3). Washington, DC.

Office of the Director of National Intelligence. (2008, October 2). *Reciprocity of Personnel Security Clearance and Access Determinations* (IC Policy Guidance 704.4). Washington, DC.

Office of the Director of National Intelligence. (2008, October 2). *Intelligence Community Personnel Security Database Scattered Castles* (IC Policy Guidance 704.5). Washington, DC.

Office of the Director of National Intelligence. (2015, February 4). *Conduct of Polygraph Examinations for Personnel Security Vetting* (IC Policy Guidance 704.6). Washington, DC.

Office of the Director of National Intelligence. (2008, June 12). *Center for Security Evaluation Construction Security Review Board* (IC Policy Guidance 707.1). Washington, DC.

Office of the Director of National Intelligence. (2012, July 25). *Application of Dissemination Controls: Originator Control* (IC Policy Guidance 710.1). Washington, DC.

Office of the Director of National Intelligence. (2014, March 20). *Application of Dissemination Controls: Foreign Disclosure and Release Markings* (IC Policy Guidance 710.2/ 403.5). Washington, DC.

Office of the Director of National Intelligence. (2015, January 29). *Acquisition Technical Amendment* (IC Policy Guidance 801.1). Washington, DC.

Office of the Director of National Intelligence. (2011, October 21). *Acquisition Workforce* (IC Policy Guidance 801.3). Washington, DC.

Office of the Director of National Intelligence. (2012, April 23). *Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities* (Memorandum). Washington, DC.

Office of the Director of National Intelligence National Counterintelligence Executive. (2012, April 23). *Technical specifications for construction and management of Sensitive Compartmented Information Facilities* (Memorandum). Washington, DC.

Oltsik, J. (2016). *Building an Enterprise Security Architecture*. Enterprise Strategy Group. Milford, MA.

Perkins, E. (2014). *20/20 Security for the Digital Business.* Gartner. Stamford, CT.

Police Executive Research Forum. (2014). *The Role of Local Law Enforcement Agencies in Preventing and Investigating Cybercrime.* Washington, DC.

Program Manager, Information Sharing Environment. (2007). *Civil Rights and Civil Liberties Protection Guidance*. Washington, DC.

Program Manager, Information Sharing Environment. (2008) *Privacy and Civil Liberties Implementation Workbook.* Washington, DC.

Program Manager, Information Sharing Environment. (2008). *Key Issues Guidance*. Washington, DC.

Program Manager, Information Sharing Environment. (2008). *Privacy and Civil Liberties Implementation Guide*. Washington, DC.

Program Manager, Information Sharing Environment. (2013). *Information Sharing Environment Annual Report to the Congress*. Washington, DC.

Program Manager, Information Sharing Environment. (2011). *Federal Resource Allocation Criteria* (ISE Guidance 112). Washington, DC.

Program Manager, Information Sharing Environment. (2010). *Final Report: Suspicious Activity Reporting Evaluation Environment*. Washington, DC.

Program Manager, Information Sharing Environment. (2008). *Nationwide Suspicious Activity Reporting Initiative Concept of Operations* (Version 1). Washington, DC.

Quirolgico, S., Voas, J., Karygiannis, T., Michael, C., Scarfone, K. (2015). *Vetting the Security of Mobile Applications* (NIST Special Publication 800-163). Washington, DC.

Rolfe, R. (2004). *Integrated Cognition- A Proposed Definition of Ingredients, A Survey of Systems, and Example Architecture* (Paper P-3855). Institute for Defense Analyses. Alexandria, VA.

Rolfe, R. (2014). *19th ICCRTS Cyber Operations Model for Multi-Domain Conflict*. Institute for Defense Analyses. Alexandria, VA.

South Florida Cyber Task Force. (2013). *Memorandum of Understanding Between FBI and the City of Miami PD.* Miami, FL.

Spidalieri, Francesca. (2015). *State of the States on Cybersecurity*. Salve Regina University. Newport, RI.

SRI International. (2009). *Networking and Information Technology Workforce Study: Final Report.* Washington, DC.

State of CA Department of Justice Office of the Attorney General. *Cyber exploitation* (n.d.). Retrieved April 20, 2016, from http://oag.ca.gov/cyberexploitation.

Steiner, J. (2009). *Improving Homeland Security at the State Level*. Central Intelligence Agency. Washington, DC.

Undersecretary of Defense, Operational Test and Evaluation (2014, August 1). *Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Processes* (Memorandum). Washington, DC.

United Nations Office on Drugs and Crime. (2013). *Comprehensive Study on Cybercrime*. United Nations. New York, NY.

Vadnais, G. (2015). *Michigan Army National Guard State of the State 2015-2025* (Presentation). Lansing, MI.

Virginia Fusion Center. (2008). *Memorandum of Understanding between the Federal Bureau of Investigation and the Virginia Fusion Center*. Richmond, VA.

Virginia State Police. (2009). *Virginia State Police*. Retrieved from http://www.vsp.state.va.us/OrgStructure.shtm

APPENDIX B: STATE LEVEL SENSITIVE COMPARTMENTALIZED INFORMATION FACILITIES

Certain information derived from intelligence sources, methods, or analytical processes is legally required to be handled within formal control systems to ensure the information's protection and integrity. This information is known as Sensitive Compartmented Information (SCI). It is the responsibility of the Director of National Intelligence (DNI) to establish formal control systems so that SCI can be handled, processed, discussed, stored safely and protected against unauthorized or unlawful disclosure. While DNI sets the policy for SCIF's and the storage, classification, processing, and release of SCI, Federal agencies derive their own policies for the handling of SCI within their organizations. These policies use the DNI Intelligence Community Directive (ICD) 705 [16] as a base, and expand upon it to suit their particular needs.

What are SCIFs? Sensitive Compartmented Information Facilities (SCIFs) are accredited areas, rooms, or buildings where SCI is stored, processed, discussed, and used to make decisions. SCIFs are only required for designated SCI material.

How are SCIFs used at the State Level? At the State Level, the establishment of SCIFs and access to SCI information is facilitated through the National Guard, which falls under DoD oversight. The Chief National Guard Bureau Instruction 2200.01 National Guard Access to Top Secret Sensitive Compartmented Information states that the Chief of the National Guard Bureau (CNGB), the Adjutants General (TAG), and their designated staff must have ready access to TOP SECRET (TS)/SCI information within one hour of notification that available information containing critical threat information exists. If a SCIF is not accessible within one hour of notification, a National Guard Joint Forces Headquarters State SCIF may be established. The policy also articulates that States will be provided access to SCIFs, and to critical threat information through information

SCIF Requirements Snapshot – Construction Security Plan

The Construction Security Plan (CSP) is one of the most critical documents that all SCIFs must have in order to achieve Defense Intelligence Agency (DIA) accreditation. The CSP is developed to address the application of security to the SCIF planning, design, and construction efforts. Even if retrofitting a SCIF that has been accredited previously, a new CSP must be developed prior to the start of work or installation and the SCIF will need to be reaccredited once construction is complete.

The CSP consists of a variety of things, which include but are not limited to: a risk assessment of threats to the project, Security in Depth documentation describing layers of protection, descriptions of adjacent facilities and activities, and site security plans, including access control, and a procurement, shipping, storage plan. An SCI-indoctrinated site security manager (SSM) is responsible for the development of the CSP and all of those components. This individual will be the single point of contact for the accrediting official (AO) regarding SCIF security. Being the Accrediting Organization, DIA has a CSP template that they will be able to provide. [3, 23]

systems and programs, classified at the TS/SCI level in support of homeland defense. Under this authority, the National Guard currently manages and maintains several SCIFs in several states.

How is a National Guard State SCIF accredited? When establishing a new National Guard Joint Force Headquarters (JFHQ) SCIF, it must be accredited by DoD, specifically the Defense Intelligence Agency (DIA), as a certified SCIF. As the Chief National Guard Bureau Instruction (CNGBI) 2200.01 states, the Army National Guard Director of Intelligence or the Air National Guard Director of Intelligence will coordinate with the State's Senior Intelligence Officer and with DIA to achieve the accreditation. [1] Derived from DNI, the DoD has specific policy on the construction, security, administration, and maintenance of SCIFs. Standards for construction and design of SCIFs are predominantly found in the Unified Facilities Criteria (UFC) 4-010-05, while the policies and procedures for SCIF administration can be found within the Department of Defense Manual (DoDM) 5105.21 Vol. 1-3. [2, 3, 4, 5, 6] All of these standards must be followed and documented in order to achieve accreditation. The Technical Specifications for Construction and Management of SCIFs Version 1.3 provides a useful guide, check list, and the various forms that must be completed in order to achieve accreditation. [26] On average, the accreditation process can take a year or more.

How is a National Guard State SCIF managed and maintained? In order for a SCIF to be operational, several roles and positions must be established and filled. The CNGBI 2200.01 identifies many of these roles at the State level. All roles require SCI-indoctrination. To start with, the TAG should appoint a State Senior Intelligence Officer (SIO) and a State Special Security Officer (SSO). The State SIO is responsible for coordinating the SCIF accreditation process with DIA, coordinating with the National Guard Bureau (NGB) to obtain TS/SCI access, and requesting security clearances and administering access for the TAG and designated staff. [1]

The State SSO manages the SCI security program and oversees all of the day to day security functions for SCIFs. The State SSO is responsible for serving as the official channel for certifying and receiving SCI visitor clearances and accesses, performing all aspects of the SCI Personnel Security Program, including, but not limited to, nomination interviews, validation of SCI access requirements, submission of investigative requests, conducting SCI security briefings; obtaining signed Non-Disclosure Agreements (NDA); and performing other related personnel security actions. For a complete listing of the SSO's responsibilities reference DoDM 5105.21 Volume 1. If an SSO is unable to be resident within a SCIF, a Special Security Representative (SSR) can be appointed to fulfill one or more of the on-site SSO responsibilities. [2]

The SSO designates a Site Security Manager (SSM) for each new SCIF construction or renovation project. The SSM is responsible for all security aspects of the SCIF construction and must develop a Construction Security Plan, a critical document for SCIF accreditation. The SSM is responsible for ensuring all construction personnel have security checks conducted and that the site is controlled and secured. [3]

Who is able to use a SCIF? Another key factor for using and operating a SCIF is understanding clearance requirements. Only those who are SCI-indoctrinated should be granted access to a SCIF. Based on the Intelligence Community (IC) policy 704.4 [22], SCI clearances have reciprocity, that is to say, an SCI clearance is recognized across all Federal agencies once the clearances is granted. An SCI clearance granted by Department of Homeland Security (DHS) will

be recognized by the DoD and the other Intelligence Community (IC) elements. ICD 705.1 also states that SCIFs have reciprocity, "Any SCIF that has been accredited by one IC element head or designee shall be reciprocally accepted by all IC elements when there are no waivers to these standards". [16]

The process for obtaining SCI access is set by IC security investigation standards in IC Planning Guidance (ICPG) 704.1 [19]. Before SCI may be granted, the applicant must have an active TOP SECRET clearance and demonstrate a requirement to access the SCI information. In order to get a TOP SECRET clearance, the applicant must first present a need to know requirement to the agency responsible for the TOP SECRET information (also known as the adjudicator). Once that is met, a Single Scope Background Investigation (SSBI) is conducted going back 10 years. Once the TOP SECRET clearance has been granted, the applicant will submit a Standard Form 86-C to an adjudicator, who then reviews the SSBI. If there are no issues, the adjudicator enters that information into the SCI database and has the applicant read into the SCI accesses.

It is important to note that although the requirements and processes for gaining access to SCI have been standardized across Federal agencies, the same is not true for CONFIDENTIAL, SECRET, or TOP SECRET clearances. A Department of Justice–Federal Bureau of Investigation (DOJ-FBI) SECRET clearance may not be recognized by or use the same systems as the DoD. This has been a recurring issue with information-sharing practices. At the state level, it will be important to understand and document who has what kind of clearance from which organizations, and ensure proper Memoranda of Understanding (MOUs) or waivers are completed to address reciprocity.

A variety of Federal agencies are able to grant clearances at the state level. The FBI has information sharing programs with local law enforcement agencies that grant clearances at the FBI SECRET and sometimes FBI TOP SECRET level. DHS is able to sponsor state officials for TOP SECRET/SCI accesses [25]. The DoD facilitates the clearances process (CONFIDENTIAL through SCI) for the National Guard. Based on the CNGBI 2200.01, the National Guard, through the DoD, is able to sponsor SCI accesses for State officials [1]. Since many of the SCIFs being built or procured at the State level are National Guard owned, obtaining SCI accesses through the National Guard may provide minimized overhead and align to the DIA accreditation requirements. For SCI however, as long as an applicant has a SSBI going back 10 years and the requisite need to know, they will be eligible to apply for an SCI and will be able to access the SCIFs, no matter the agency.

Based on the U.S. Office of Personnel Management (OPM) billing rates for investigations, a standard SSBI investigation costs $5,188 (base). Reinvestigations for SCI accesses are required every five years [24].

What are the actions/timelines that need to be followed? In order to operate a SCIF at the state level, certain things must be done prior to receiving the SCIF, once the SCIF is received, and then when in maintenance. The items below are a starting point:

- Prior to Receiving the SCIF:
  - Ensure people with SCI clearances are in place for receiving and connecting the SCIF.
    - Ensure SIO, SSO, SSM (and others as required) are identified.
  - Complete a construction site plan.
  - Plan the accreditation process.

  - Review TEMPEST Requirements in accordance with National Telecommunications and Information Systems Security (NTISS) documents. [27, 28, 29, 30, 31, 32, 33]
  - Establish a process for obtaining clearances and a reciprocity process.
- Once SCIF is Received:
  - Implement construction site plan.
  - Follow other accreditation requirements:
    - Determine and write policies for the SCIF.
    - Conduct a TEMPEST evaluation.
    - Implement Access Control process and Intrusion Detection Systems.
  - Complete Approval to Operate (ATO) documentation for the various networks that are planned to be installed and operated within the SCIF.
  - Determine how many resources are needed.
  - Formalize an MOU for stakeholders expected to participate (assuming clearances are in place).
- SCIF Operations and Maintenance:
  - Conduct periodic facility evaluations.
  - Complete clearance reinvestigations every five years.

References

(1) Chief National Guard Bureau (2015, November 16). *National Guard Access to Top Secret Sensitive Compartmented Information* (CNGB Instruction 2200.01). Washington, DC

(2) Department of Defense. (2012, October 19). *Sensitive Compartmented information (SCI) Administrative Security Manual: Administration of Information and Information Systems Security* (DoD Manual 5105.21 Volume 1). Washington, DC.

(3) Department of Defense. (2012, October 19). *Sensitive Compartmented information (SCI) Administrative Security Manual: Administration of Physical Security, Visitor Control, and Technical Security* (DoD Manual 5105.21 Volume 2). Washington, DC.

(4) Department of Defense. (2012, October 19). *Sensitive Compartmented information (SCI) Administrative Security Manual: Administration of Personnel Security, Industrial Security, and Special Activities* (DoD Manual 5105.21 Volume 3). Washington, DC.

(5) Department of Defense (2013, October 1). *Sensitive Compartment Information Facilities Planning, Design, and Construction* (Unified Facilities Criteria 4-010-05). Washington, DC.

(6) Department of Defense (2015, July 8). *DoD Facilities Pricing Guide* (Unified Facilities Criteria 3-701-01). Washington, DC.

(7) Department of Homeland Security. (2004, September 17). *Sensitive Compartmented Information Program Management* (DHS Management Directive 11043). Washington, DC.

(8) Department of the Air Force. (2015, November 13). *Criminal Investigations and CI* (AF Policy Directive 71-1). Washington, DC.

(9) Director of Central Intelligence. (2002). *Physical Security Standards for Sensitive Compartmented Information Facilities* (CIA Directive 6/9). Washington, DC.

(10) Director of Central Intelligence. (1994). *Physical Security Standards for SCIFs* (CIA Directive 1/21). Washington, DC

(11) Executive Office of the President. (2007). *National Strategy For Information Sharing: Successes and Challenges in Improving Terrorism-Related Information Sharing*. Washington, DC.

(12) Executive Office of the President. (2012). *National Strategy for Information Sharing and Safeguarding*. Washington, DC.

(13) Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108-458, 118 Stat. 3638, codified as amended at 50 U.S.C. § 401 et seq.

(14) National Guard Association. (2010). *NGAUS Fact Sheet: Understanding the Guard's Duty Status*. Washington, DC.

(15) National Guard Association. (2015). *Legislative Objectives for Preparation of Fiscal Year 2016 Defense Budget*. Washington, DC.

(16) Office of the Director of National Intelligence. (2010, September 17). *Physical and Technical Security Standards for Sensitive Compartmented Information Facilities* (IC Standard 705.1). Washington, DC.

(17) Office of the Director of National Intelligence. (2013, June 21). *Protection of Classified National Intelligence, Including SCI* (IC Directive 703). Washington, DC.

(18) Office of the Director of National Intelligence. (2009, June 10). *Reciprocity for Intelligence Community Employee Mobility* (IC Policy Guidance 709). Washington, DC.

(19) Office of the Director of National Intelligence. (2008, October 2). *Personnel Security Investigative Standards and Procedures Governing Eligibility for Access to SCI and other Controlled Access Program Information* (IC Policy Guidance 704.1). Washington, DC.

(20) Office of the Director of National Intelligence. (2008, October 2). *Personnel Security Adjudicative Guidelines for Determining Eligibility for Access to Sensitive Compartmented Information and other Controlled Access Program Information* (IC Policy Guidance 704.2). Washington, DC.

(21) Office of the Director of National Intelligence. (2008, October 2). *Denial or Revocation of Access to Sensitive Compartmented Information, other controlled Access program Information and Appeals Processes* (IC Policy Guidance 704.3). Washington, DC.

(22) Office of the Director of National Intelligence. (2008, October 2). *Reciprocity of Personnel Security Clearance and Access Determinations* (IC Policy Guidance 704.4). Washington, DC.

(23) Office of the Director of National Intelligence. (2012, April 23). *Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities* (Memorandum). Washington, DC.

(24) United States Office of Personnel Management. (2015, October 2). *Investigations Reimbursable Billing Rates Effective October 1, 2015* (Federal Investigations Notice No. 16-01). Washington, DC.

(25) Department of Homeland Security. (2009, June). *The Department of Homeland Security Personnel Suitability and Security Program* (DHS Instruction Handbook 121-01-007). Washington, DC.

(26) Office of the Director of National Intelligence. (2015, September 10). *Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities* (IC Tech Spec for ICD/ICS 705 v.1.3). Washington, DC.

(27) NACSIM 5100A *Compromising Emanations Laboratory Test Requirements, Electromagnetics. National Security Telecommunications and Information System Security (NSTISS)*

(28) NTISSI 7000 *National Telecommunications and Information Systems Security Instruction, TEMPEST Countermeasures for Facilities, 7 October 1988*

(29) NTISSP 300 *National Telecommunications and Information Systems Security Policy, National Policy on the Control of Compromising Emanations, 3 October 1988*

(30) NSTISSAM *Compromising Emanations Laboratory Test Requirements,*

(31) TEMPEST/1-92 *Electromagnetics. National Security Telecommunications and Information System Security (NSTISS)*

(32) National Security Agency. (1987, August 31). *Commercial COMSEC Endorsement Program Procedures.*

(33) National Security Agency. (1990, October). *INFOSEC System Security Products & Services Catalog.*

APPENDIX C: GOVERNANCE

Governance, which establishes leadership mechanisms, is a crucial element in meeting Cyber Hub objectives. An overarching Governance strategy and implementation plan provides the foundation for an organizational construct empowered as the approval and directive authority for all cyber and information technology for the State CIO, with operational feedback from stakeholders. Key stakeholders can prioritize critical infrastructure cyber issues within this framework.

A Charter Agreement and Memoranda of Understanding can clearly establish the organizational construct and define oversight roles and responsibilities for subscribing members and stakeholders. Because structures across each state vary and authorities may not be aligned, an additional decision point for consideration, based on a state's legislation, is whether or not the sample Cyber Hub Management Construct charter (see Appendix D) can be modified for adoption. The ideal construct is centralizing decision-making at the state level to achieve the synergy required among stakeholders.

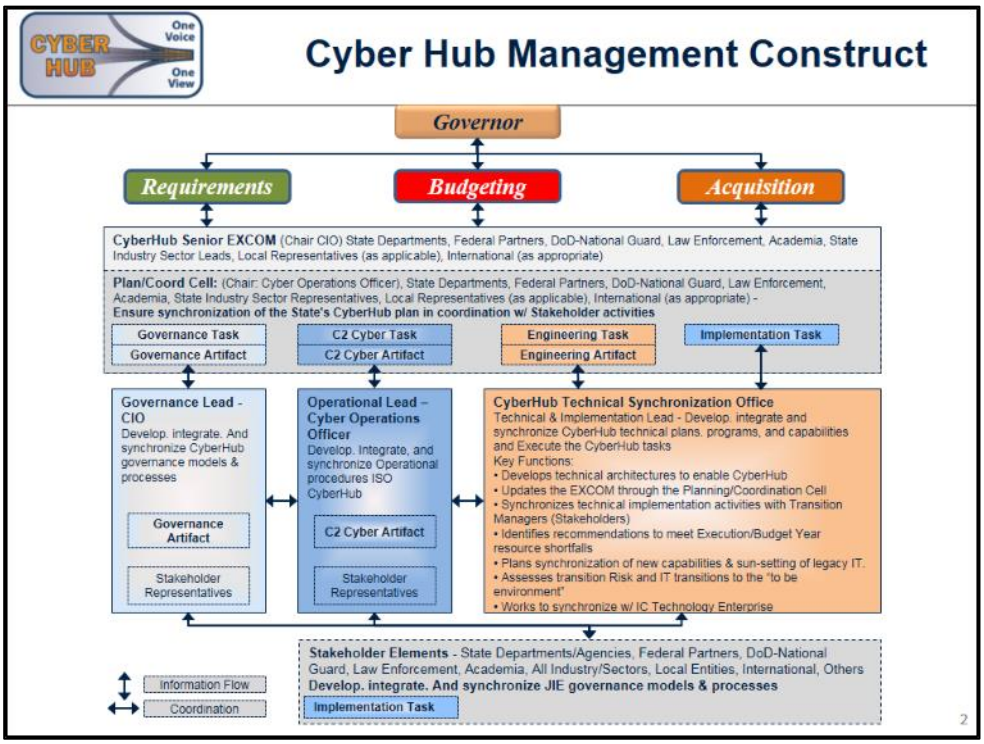


Figure C-1: Sample Cyber Hub Management Construct

Figure C-1, above, illustrates the environment and the interrelationships among stakeholders, functions, and processes, which are described in the three fundamental elements for enabling follow-on actions.

- A single authority empowered as the approval and directive authority for all Cyber/IT for the State CIO with operational feedback from Stakeholders:

  - A single authority to prevent duplication of Cyber/IT capabilities across all Mission Areas,
  - A single oversight authority for provisioning the Cyber Hub,
  - A single authority to operate the Cyber Hub,
  - Approval required for any deviation for non-compliance,
  - Requirements/Analysis of Alternatives (AoA),
  - Enterprise solutions must be evaluated, and
  - Justifications developed when they are not used;

- Transparent and active oversight of state-wide Cyber/IT budget formulation and execution:
  - Controlling the funding of capabilities is critical to the execution of the entire effort,
  - State CIO, together with Comptroller and Auditor General,
  - Integrating Cyber/IT budgets across all Stakeholder Components,
  - Ensure guidance is reflected in Component Programmed Budget submissions, and
  - Balances cost, schedule, and performance;

- Single authoritative and enforced State Information Enterprise Architecture to define:
  - Information Enterprise capabilities,
  - Reference Architectures,
  - Cyber/IT standards, and
  - Compliance criteria.

Background

The DoD CIO initiated a Department-wide effort to establish a secure Joint Information Environment (JIE), comprising shared information technology (IT) infrastructure, enterprise services, and a single security architecture to achieve full-spectrum superiority, improve mission effectiveness, increase security, and realize IT efficiencies. This effort required a common framework the ensure the JIE could be operated and managed per the authorities and responsibilities specified in the Unified Command Plan (UCP) (current and future) using enforceable standards, specifications, and common tactics, techniques, and procedures (TTPs). The end result was a management construct that enabled disparate organizations to have a common platform in order to advise and inform the DoD CIO on the full range of statutory and regulatory matters pertaining to IT Investments, Cybersecurity (CS), Spectrum, Command and Control, Enterprise Infrastructure, Information Management, IT/CS Workforce, and Cyber. It provides unified strategic direction and advice to efficiently manage, secure, and operate the JIE across all IT and Mission systems with all operational environments.

The JIE Management Construct (JMC) can be directly applied at the state level to create an example Cyber Hub Management Construct (CMC) to synchronize implementation and operations. It will improve Cyber Hub Operations by directly involving all stakeholders in oversight, planning, and advocacy to enable the ability to assess shortfalls; identify, validate, and implement viable, affordable enterprise-wide solutions. The CMC's mission can be summarized as:

- Assess unmet Cyber Hub requirements / develop alternative options,

- Rapidly acquire / field Cyber Hub capabilities,
- Identify and overcome bottlenecks and barriers,
- Adapt to evolving requirements,
- Pursue innovative solutions to Cyber Hub challenges,
- Coordinate and operationalize Cyber Hub Initiatives,
- Speed deployment and enhance operational capability, and
- Develop prime objectives in evaluating options.

The sample converted JMC Charter that is attached in Appendix D can be modified and adjusted to address specifics for a given state's unique mission sets and stakeholders to establish a CMC charter.

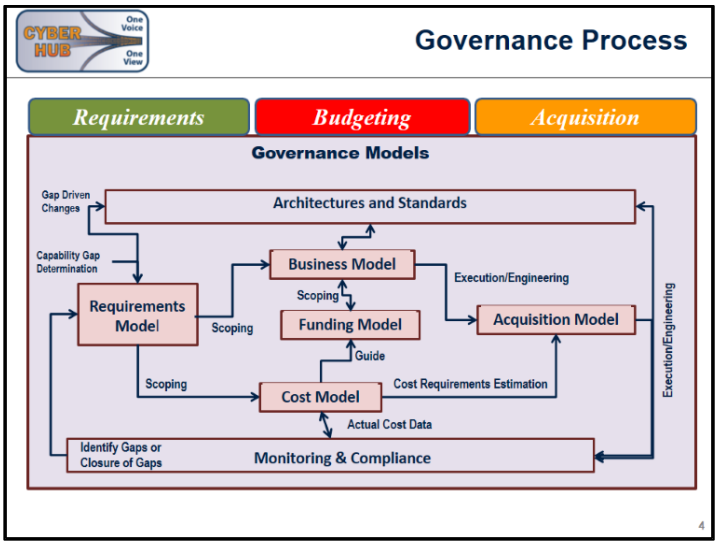


Figure C-2: Governance Process

Prioritized requirements based on capability gaps submitted by Stakeholders drive the governance process throughout the Cyber lifecycle. The governance interrelationships are critical to the timing and successful delivery of capabilities to the Cyber Hub, as seen in Figure C-2. The elements needed for each step of the process are:

1. Governance Model – Establish structures and processes for setting direction, establishing standards, enforcing compliance, and prioritizing Cyber/IT investments.
2. Strategic Communications – Develop high-level Governance
3. Requirements Model – Establish integrated structures and processes that optimize Cyber Hub inputs in the State Requirements process in support of Cyber/IT requirements validation.
4. Business Models – Establish a State-wide approach for common Cyber/IT business needs and direct Cyber/IT related business and operational practices that will deliver operational effectiveness, cyber security, and economic efficiencies to the Cyber Hub.
5. Costing Models – Establish various standard methodologies for determining the total cost of ownership and for supporting State-wide decision-making.
6. Funding Models – Establish a State-wide common framework for determining Cyber/IT Funding approaches in accordance with Planning, Programming, Budgeting, and Execution

(PPBE) to reduce acquisition, procurement, and sustainment expenditures; improve Cyber/IT cost awareness; eliminate redundancy.

7. Acquisition Model – Establish integrated structures and processes that optimize acquisitions systems support of Cyber Hub acquisitions.

Technology Impact on Governance

As cyber technologies evolve, the decision cycles between strategic governance and operational governance (down to an individual capability/project) begins to shrink, allowing cyber responses to be implemented tactically while still achieving strategic objectives (see Figure C-3).

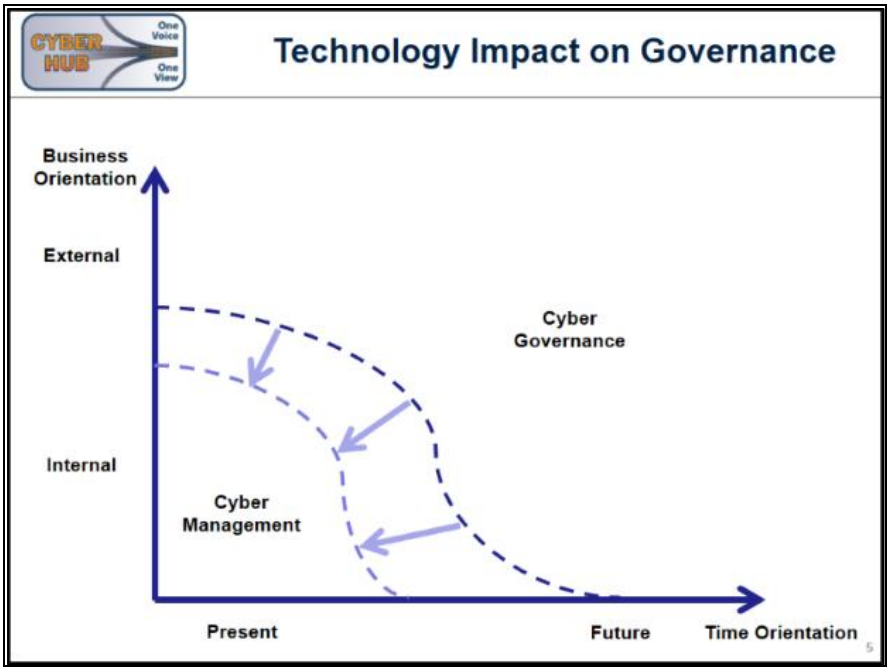


Figure C-3: Technology Impact on Governance

The key elements between Strategic (Cyber Governance) and Operational (Cyber Management) are identified in the table below.

Cyber Governance	Cyber Management
Define, establish and align the Cyber/IT governance framework with the overall enterprise governance and control environment.	Establish a project management approach commensurate with the size, complexity and regulatory requirements of each project.
Base the framework on a suitable Cyber/IT process and control model and provide for unambiguous accountability and practices to avoid a breakdown in internal control and oversight.	The project governance structure can include the roles, responsibilities and accountabilities of the program sponsor, project sponsors, steering committee, project office and project manager, and the mechanisms through which they can meet those responsibilities (such as reporting and stage reviews).
Confirm that the Cyber/IT governance framework ensures compliance with laws and regulations and is aligned with, and confirms delivery of, the enterprise's strategies and objectives.	Make sure all Cyber/IT projects have sponsors with sufficient authority to own the execution of the project within the overall strategic program.
Report Cyber/IT governance status and issues.	Report Cyber/IT governance status and issues.

Governance Framework

Control Objectives for Information and Related Technology (COBIT) was the framework used to hierarchically distinguish tasks from the strategic level down to the tactical level to enable organizational decision-making. The tasks can then be aligned across the life-cycle processes, as seen in Figure C-4.

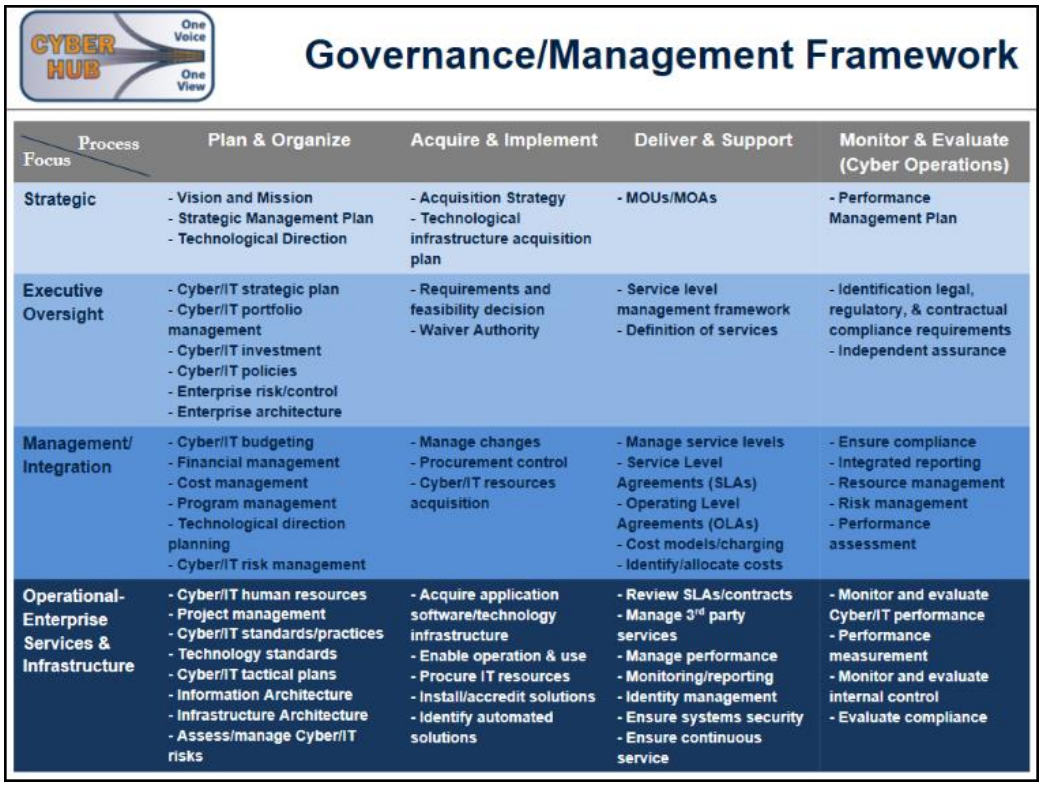


Figure C-4: Governance/Management Framework

This page intentionally left blank.

APPENDIX D: SAMPLE CYBER HUB MANAGEMENT CONSTRUCT CHARTER

I. PURPOSE AND SCOPE:

1. This charter is established under the authorities of the Governor of the State to move State Departments, Agencies, and private and public stakeholders to the State Cyber Hub Operations.

2. This document establishes the Cyber Hub Management Construct (CMC). The CMC is an organizational and functional framework that establishes activities; defines roles and responsibilities; and specifies processes for implementing, governing, and administering the Cyber Hub strategy. Cyber Hub processes synchronize the Stakeholders Plans of Action and Milestones (POA&Ms) and execution activities while ensuring alignment with the overall State's Cyber Hub effort.

3. The CMC is also responsible for identifying compliance issues and making recommendations on resource, requirements and funding shortfalls through the CIO to the Requirements, Budgeting, and Acquisition processes and to the respective Component Stakeholders for resolution. If the Component Stakeholders can resolve the problem, then the CMC will continue to implement the Cyber Hub Operations plan. However, when resolution within the Stakeholders is not possible, conflicts will be elevated to the appropriate senior governing body for requirements, budgeting, acquisition, operations, and Cyber/IT within the State for resolution.

4. The CMC will coordinate implementation actions with the potential to impact ongoing operations with transition managers, who coordinate with the Operational Sponsor and Cyber Technical Synchronization Office (CTSO) to ensure continuity of operations (COOP). For conflicts, the issues will be escalated to the Cyber Senior Executive Committee (EXCOM) for resolution.

II. BACKGROUND:

1. The Cyber Hub is defined as the operational decision support capability (engine) for cyber operations within the State.

2. The objective of the Cyber Hub is to provide the common operating picture (COP) based on operationalized information and intelligence from disparate sources using advanced analytics to provide near real time cyber decision response capabilities across the State’s cyber ecosystem for use by Departments, Agencies, and public and private mission partners in all operational environments. The Cyber Hub will support the full range of State operations through Federal defense of the State’s Information Network against kinetic and non-kinetic attacks while at the same time supporting business, government, and intelligence operations of the State.

SAMPLE

3. In addition, Cyber Hub operations supports Homeland Defense and Defense Support of Civil Authorities operations and enables the State and other interagency mission partners to seamlessly share vital information. The Cyber Hub also supports humanitarian assistance/ disaster relief, law and peace enforcement, peacekeeping, and show of force operations in addition to supporting multi-national operations, exercises, and training.

4. The governance, operational and technical characteristics need to be approved as a means of scoping and clarifying the activities of Cyber Hub Operations and to provide the boundaries for achieving the objectives of the Cyber Hub. The characteristics that should be agreed upon for the CMC are listed below:

- Network enables mission success in all domains to include agile safe sharing with mission partners.
- Agency and industry stakeholders retain mission-specific applications when critical for mission success.
- Allows integration and execution of cyberspace capabilities within, through and across the other Critical Infrastructure Sector domains.
- Network is centrally managed, but de-centrally executed.
- Pre-planned procedures/Cyber Rules of Engagement enable decisions at the lowest level.
- Common Operating Picture as depicted in an Information Technology Enterprise Strategy and Roadmap.
- Command and Control (C2) Concept of Operations (CONOPS) describes State Departments, Agencies, public and private partners' engagement in Cyber Hub to enable joint information sharing through a centralized Cyber Hub organization.
- Fully optimized set of State enterprise-level data & operations centers.
- Shared situational awareness for all Cyber/IT activities.
- Shared Cyber/IT Infrastructure.
- Common Enterprise Services, Applications and Tools.
- Shared services are established to support timely and secure access to protected data and applications.
- Global Authentication and Directory Services fully interoperable with Intelligence Community (IC) and interagency mission partners.
- Foundational and shared common services are globally available and accessible at the tactical edge.
- Access at the point of need.
- Common Identity Management and Access Control fully interoperable with IC and interagency mission partners.
- Single Security Architecture.
- The State network and security architecture replaces current Stakeholder-specific architectures.
- Data Centric vice Net-Centric.
- The ability to use velocity, value, variety, and volume of data improves decision-making and situational awareness.
- Cyber Hub-approved non-standard interfaces (transport and application layer) allow Component Stakeholders to support mission-unique requirements seamlessly in a joint/ combined environment.

SAMPLE

- Forces in a disconnected, intermittent, low-bandwidth environment maintain the capability to execute mission-critical functions.
- Initial-entry expeditionary capabilities supported by Cyber Hub.
- Mission assurance (e.g., COOP) is inherent in the design of Cyber Hub Operations.

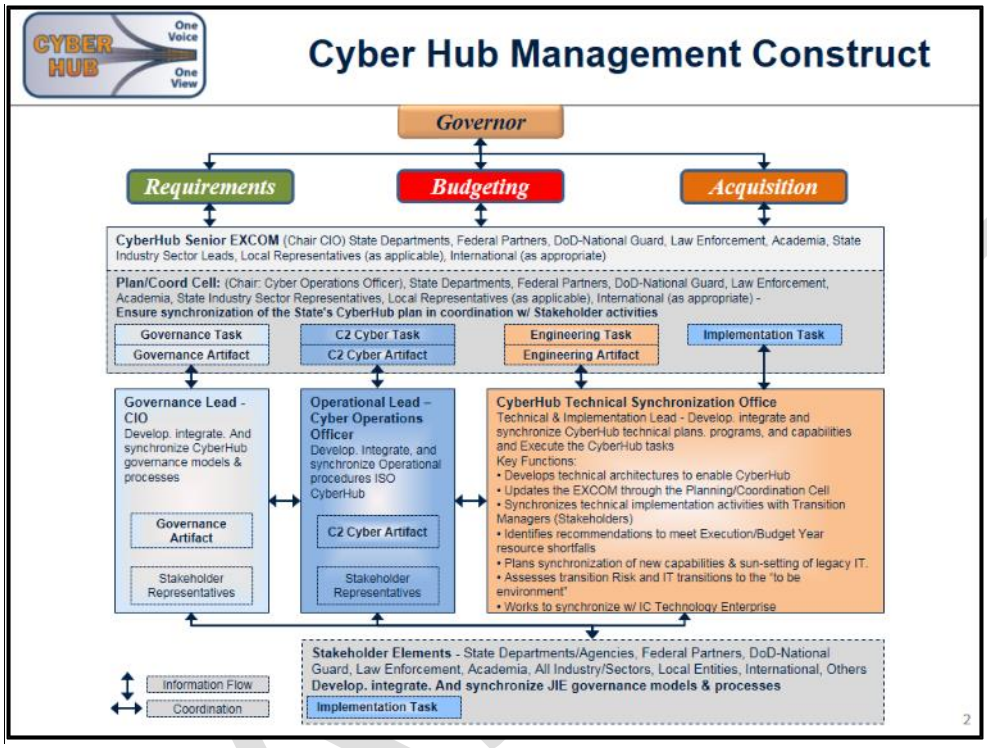


Figure D-1: Governance/Management Framework

1. Figure D-1 depicts the overall Cyber Hub governance structure. At the strategic level, the figure depicts the alignment of Cyber Hub with key State processes. Cyber Hub related requirement decisions will be validated by the "State Requirements process"; Planning, Programming, Budgeting, and Execution (PPBE) decisions will be approved at the "State Financial process"; and acquisition decisions through "State Acquisition process". Additionally, operational decisions are made at the Cyber Hub. The CIO is charged with making State-level recommendations on Cyber/IT related policy, budgetary and acquisition decisions as well as leading the overall Cyber Hub initiative. Sections 1 through 7 below highlight the functions of the Cyber Senior Executive Committee and the subordinate CMC structure.

2. Cyber Senior Executive Committee (EXCOM):

- Sets the Cyber Hub direction, establishes goals and objectives, and provides oversight and maintains accountability.
- Develops Cyber Hub plans, policies and governance approaches; initiates review of issues, IT related programs, initiatives and systems considered essential for enterprise-wide solutions and operational effectiveness; provides Cyber Hub standards; recommends investments and enforces compliance.

- Provides decisions on the Cyber Hub execution plan. Elevates operational issues through the Chief Information Officer (CIO) to "State Operations Board" in coordination with the State's Technical Department Lead.
- Elevates resourcing issues through the CIO to the "State Financial Board" up to the Governor for decision. Elevates acquisition issues to the Chief Acquisition Executive for review and /or decisions.
- Authorizes additional permanent and temporary working groups, as necessary, to facilitate execution of Cyber Hub tasks.

3. Cyber Hub Planning and Coordination Cell: Ensures the synchronization of Component Stakeholder actions to realize an integrated State-wide implementation of the Cyber Hub.
   - Coordinates Component and leadership updates.
   - Maintains the Integrated Master Schedule, tracks Implementation Plan and maintains overall Cyber Hub CONOPS.
   - Synchronizes Plan of Actions and Milestone (POA&M) compliance with the Components' activities.
   - Ensures the coordination and synchronization of activities of the Governance, Operational, and Technical elements.
   - Coordinates resource planning, execution and Unfunded Requirements tracking.
   - Manages implementation issue resolution and execution on behalf of the Cyber Senior EXCOM as depicted in Section I, paragraph 3 above.
   - Develops and publishes standardized Cyber Hub Strategic Communications.

4. Governance planning group should have oversight and authority to develop, integrate, and synchronize efforts for all stakeholders
   - Provides the overarching plans, guidance, and policy that inform requirements approval, Enterprise Architectures development and State Cyber processes
   - Coordinate planning and resourcing activities
   - Review Service Level Agreements (SLAs) and/or Memoranda of Agreement (MOAs)
   - Update to the senior executive committee through a planning and coordination body

5. Operational group would develop, integrate and synchronize operational procedures with state- and federal-level procedures
   - In coordination with execution leads, coordinate and lead development of C2 Cyber Hub construct/implementation:
   - Tactics, Techniques and Procedures (TTPs) and Standard Operating Procedures (SOPs)
   - Operations (OPS) Center accreditation process
   - Concept of Operations
   - Configuration of Enterprise Management Services (EMS) tools
   - TTPs necessary to operate and maintain Authoritative Data Repository for operational related artifacts.
   - Monitor and report on operations
   - Assess operational risk
   - Monitors SLA performance and track metrics
   - Enforce operational compliance

SAMPLE

- Oversees development of and synchronizes Continuity of Operations (COOP) and Disaster Recovery (DR) plans
- Identifies and makes recommendations on budgetary priorities, necessary for Cyber Hub operations, through the State Cyber Management Construct in coordination with mission priority lists and cyber stakeholder inputs
- Update to the senior executive committee through a planning and coordination body

6. The Cyber Technical Synchronization Office serves as the Technical and Implementation lead and provides engineering and solution architectures. They should develop, integrate and synchronize technical plans, programs, and capabilities to realize and integrate State-wide implementation of the Cyber Hub. The technical planning group should:

- Lead the development of technical specifications to enable Cyber Hub capabilities
- Serve as the Technical Configuration Manager
- Make recommendations to meet Execution/Budget Year resource shortfalls
- Plan synchronization of new capabilities and sun-setting of legacy cyber/IT capabilities
- Conducts Transition Risk assessments and synchronizes IT transitions to the "to be" environment.
- Ensures key enterprise services are aligned and interoperable to allow information sharing with the IC Information Technology Enterprise.
- Leads development of Technical Designs and Specifications.
- Provides input into Capability Requirements Documents (CRD).
- Develops Implementation plan(s) and synchronizes implementation activities with Transition Managers (State Components).
- Leads technical surveys, assessments, and reviews.
- Assesses technology innovation and insertion process.
- Leads development of Data Repository structures to enable storage of Cyber Hub related artifacts.
- Provides Technical input to Business Case Analyses (BCAs) and Analysis of Alternatives (AOAs).
- Provides Enterprise contracting capabilities.
- Maintains service catalogues.
- Manages Cyber Hub -related SLAs and MOAs.
- Coordinates activities with governance and operational activities as appropriate.
- Ensures security architecture development is designed to secure the infrastructure, provide access and allow data sharing across the environment.
- Update to the senior executive committee through a planning and coordination body

SAMPLE

7. Implementers (Component Stakeholders): Engineer, implement, and operate the Cyber Hub for their respective organizations to move the State closer to the delivery of Cyber Hub capabilities. They also identify obstacles and issues that may impede delivery of Cyber Hub capabilities and recommend solutions. Each organization will appoint a Transition Manager, who manages implementation and ensures continuity of operations as organizations transition from the "as is" to the "to be" in coordination with the theater-level execution sponsor.

- Identifies issues, risks, and obstacles to the Cyber Hub EXCOM through the Planning and Coordination Cell.
- Develops the Component's POA&M and provides input to the overall State's POA&M.
- Participates in required Cyber Hub working groups.
- Provides Cyber Hub status updates.
- Manages Cyber Hub resources for funding execution.
- Provides input to implementation plans.
- Develops the specifics plans and ensures execution of COOP and DR plans

IV. MEMBERS ROLES AND RESPONSIBILITIES: (Voting and non-voting designations apply at all levels of the Cyber Hub Governance process.)

1. CIO: Provides overall governance and direction for Cyber Hub Implementation. Chairs the Cyber Hub Executive Committee and the Cyber Hub Planning and Coordination Cell. Voting member.

2. Chief Acquisition Executive: Exercises Decision Authority for Cyber Hub, unless delegated, and subsequently approves the appointment of a Component Acquisition Executive. Voting member.

3. Chief Comptroller and Chief Financial Officer (CFO): Provides the overall Financial Management Framework and guidance for resourcing the Cyber Hub through the State's PPBE processes, to include overseeing the financial policy and the use of the financial management systems. Voting member.

4. Law Enforcement/Department of State Police: Synchronizes Intelligence Community, civil and criminal efforts with the Cyber Hub architecture and stakeholder solution architectures to ensure global operations are adequately planned and exercised. Serves as Intelligence advisor to Cyber Hub. Voting member.

5. Chief Human Resources: Serves as the Total Force Management advisor as it relates to readiness; National Guard and Reserve Component Affairs; health affairs; training; personnel requirements and management to include equal opportunity. Morale, welfare, recreation, and quality of life matters to the Cyber Hub. Synchronizes total force management automation capabilities, operations and governance with Cyber Hub. Voting member.

SAMPLE

6. Cyber Operations Officer. Serves as the Operational Sponsor and Mission Area advisor for the Cyber Hub. Chairs the Cyber Hub Planning and Coordination Cell. Synchronizes Cyber Hub processes and automation operations. Voting member.

7. Office of the Auditor General: Provides the overall State-level analytical framework for evaluation of plans, programs and budgets through the State's PPBE processes. Voting member.

8. Local Representative: Serves as an Advisor to the Cyber Hub as applicable to address social/user community impacts. Voting member.

9. Technical Lead: Leads the Cyber Hub Technical Synchronization Office and serves as the Technical and Implementation Lead for incremental delivery of Cyber Hub capabilities. Voting member.

10. International: Serves as an Advisor to the Cyber Hub where appropriate. Non-voting member.

11. Academia: Serves as the Education Advisor and recommends Cyber innovation capabilities. Voting member.

12. Industry: Implements the tasks necessary to execute the Cyber Hub plan, recommends Cyber innovation capabilities, and serves as the Transition Managers. Voting members: Sector Leads

13. National Guard: Responsible for setting the priority of activities and ensuring alignment of the State's approved strategic plan of action and milestones with operations to produce a state/regional level implementation schedule and plan. Voting member. (The Cyber Hub EXCOM will ensure that the PCC, Governance, Operations, and CTSO have established processes on behalf of the National Guard to enable participation and review for technical, operational, and governance decisions and conflict resolution. The CIO will ensure all National Guard equities are considered, represented, and factored into all Cyber Hub decisions.)

V. TIMELINE: Effective on date of signature. Duration is until a formalized State Cyber/IT governance structure is established.

VI. RESOURCING: This charter does not constitute an agreement to transfer funds or Full Time Equivalents (FTEs). A separate agreement must be developed to define the details for manpower allocations and funds necessary for participation within the Cyber Hub. Signatory stakeholders agree to pay subscription dues and provide access to data sources to support Cyber Hub operations. Cyber Hub operations provides:

    1) CONOPS
    2) Knowledge-base access
    3) Playbook access
    4) Constant observation

SAMPLE

5) As a Service
6) Hub – Organizational construct/structure and governance
7) Training

SAMPLE

APPENDIX E: INFOGRAPHICS

This page intentionally left blank.

.

State Cyber Hub Operations
Decision Support Model

Decision support is the core function of the Cyber Hub's mission. The ability to operate, organize, anticipate, and respond to an event from initial situational awareness through restoration and feedback capture requires a capability that can be undertaken only with the adoption of an operational model based on common processes and standards. It will require, at a minimum, best-of-breed processes, state-of-the-art data grooming, and an agile decision support framework. The framework enables understanding of an evolving cyber situation resulting from continuous observation across all critical infrastructure sectors.

A shared common operating picture (COP), based on current and predictive analytic capabilities, will encourage collaboration among participating stakeholders—Federal, State, local, law enforcement, industry, National Guard, and international partners in and around the Cyber Hub. Using a coherent data-driven methodology, Hub operators will inform, assess, and adapt potential responses to a cyber scenario to local, accountable decision makers, enabling them to act with the broadest of information and intelligence available at the time. Decision-making occurs in a recurring cycle of Observe-Orient-Decide-Act (OODA loop) within the Hub to inform potential response scenarios. It is critical to note that the Human-in-the-Loop (HITL) processes dominate cyber operations decisions at each stage of response.

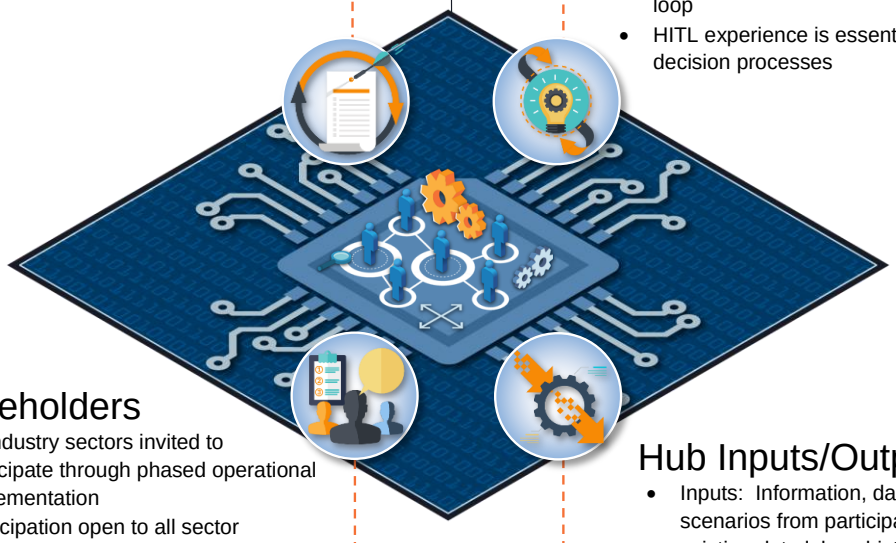
GOAL: Design and implement a decision support capability, with a shared common operating picture, leveraging existing detection/ response organizations and structures.

Purpose

- Operate, organize, and respond to an event from initial situational awareness to resolution
- Provide decision support framework and analytic outputs/ products to stakeholders via a shared COP
- Provide continuous cyber observation

Decision Support Framework

- Utilize OODA loop decision making framework to enable dynamic decision support
- Work with key stakeholders to build and utilize analytic and COP dashboard to fuel existing operations centers (as-a-service capability delivery)
- Create and test use case scenarios inside the loop
- HITL experience is essential to each phase of decision processes



Stakeholders

- All industry sectors invited to participate through phased operational implementation
- Participation open to all sector stakeholders (federal, state, local, industry, academia, international, law enforcement, and others) on a subscription, as-a-service basis
- Requirement: Charter signature (framework agreement)
- Requirement: Participation subscription fee with agile payment options (access to COP, playbook, training)

Hub Inputs/Outputs

- Inputs: Information, data, intelligence, historical scenarios from participating stakeholders, existing data lakes, historical/exercise outcomes, ongoing and real time situations for analysis
- Outputs: Ever evolving cyber knowledge base (playbook), state of constant observation, continuous learning via playbook, continuous training scenarios, shared COP
- Other: Operational construct to organize, decision support framework, governance framework

This page intentionally left blank.

INSIDE THE LOOP
Decision Support Model

Decision-making is a recurring cycle of: Observe – Orient – Decide – Act. The "OODA Loop," as it has come to be known, is a model for understanding decision-making as an iterative process whereby a decision is reached through observing an evolving situation, orienting and reorienting based on those observations, developing a response plan based on continuous observation and orientation, and then executing the decided action. Each element of the OODA Loop feeds information forward and provides feedback to the others while embracing and interacting with the environment itself. The cyclical nature of both the overall process and the iterative interactions among the elements allows the OODA Loop decision support model to evolve decisions as situations develop. Cyber events may not be static, so decision-making must not be static either.

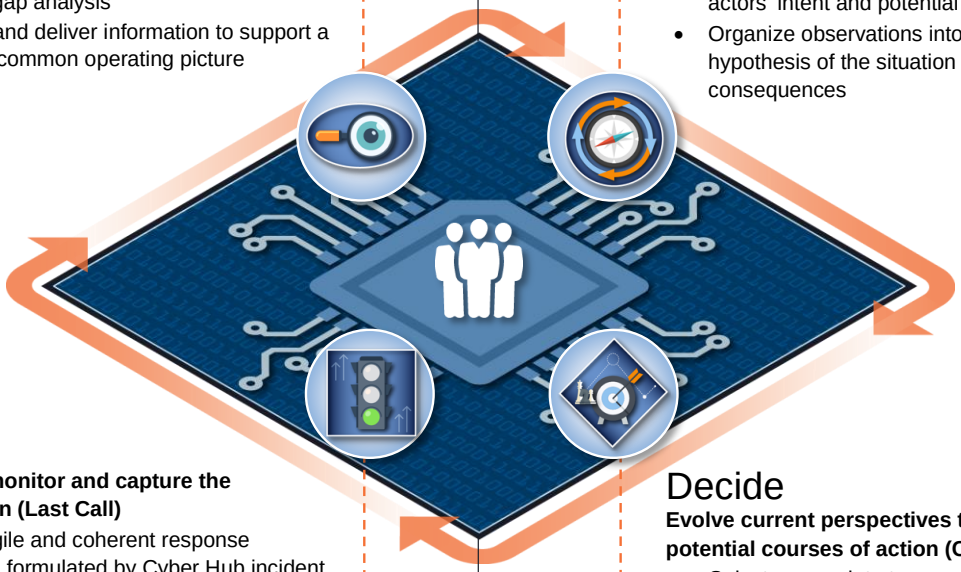
GOAL: Identify and adopt a decision support model as the basis for the Cyber Hub Concept of Operations (CONOPS).

Observe
Receive Information and Data

- Ingest intelligence and information from multiple sources
- Groom data for content via Human-in-the-Loop (HITL) and technology capabilities, and conduct gap analysis
- Prepare and deliver information to support a dynamic common operating picture

Orient
Provide context and understanding to information from Observe Element

- Categorize type of cyber event and identify prior relevant knowledge and processes
- Identify patterns of behavior and cyber actors' intent and potential attribution
- Organize observations into a working hypothesis of the situation and possible consequences



Act
Implement, monitor and capture the response plan (Last Call)

- Provide agile and coherent response operations formulated by Cyber Hub incident response team
- Continually observe operations including risk assessment, cyber alerts, and network operations
- Update dynamic and adaptive playbook for current and future decision support
- Track and report key performance indicators in order to drive ongoing operations monitoring and continuous process improvement

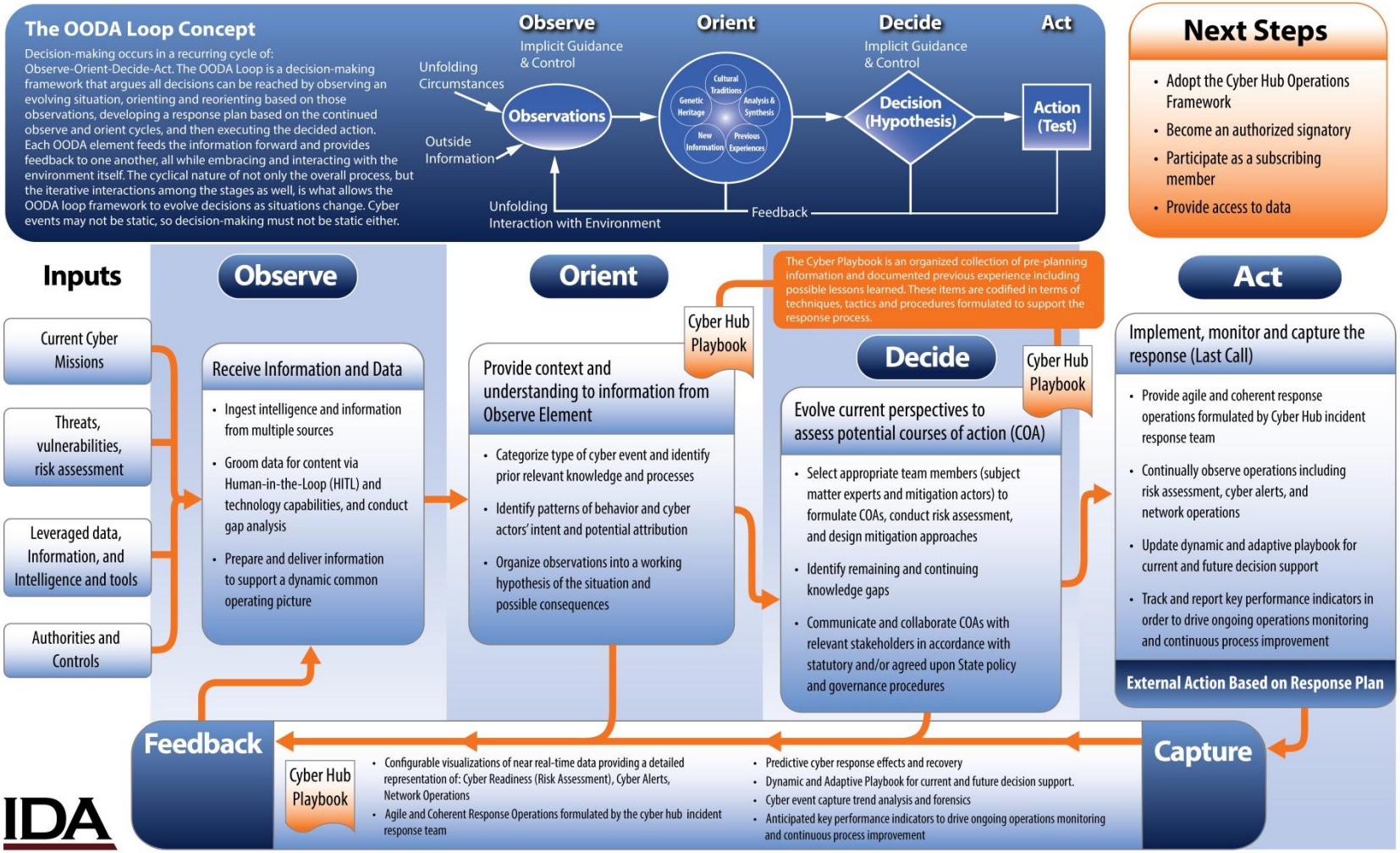
Decide
Evolve current perspectives to assess potential courses of action (COA)

- Select appropriate team members (subject matter experts and mitigation actors) to formulate COAs, conduct risk assessment, and design mitigation approaches
- Identify remaining and continuing knowledge gaps
- Communicate and collaborate COAs with relevant stakeholders and act according to statutory and/or agreed upon State policy and governance procedures

OBJECTIVES

- **OBSERVE:** Recognize significant activities within the environment, as best as possible within the available resources, and provide that information and assessment in near real-time to local decision-makers.
- **ORIENT:** Enable Cyber Hub operators and stakeholders, co-located physically or virtually, to structure decision-making processes with context knowledge and previous experience.
- **DECIDE:** Determine potential COAs based on current perspectives of the Cyber Hub team and analytic products produced by technology capabilities.
- **ACT:** Execute the COA and monitor, capture, and assess outcomes.

Cyber Hub Decision Framework - OODA Loop



Cyber Hub Technology
Cyber Dashboard

The Cyber Dashboard delivers a current and predictive data analytics capability for state networks and computer assets. It provides an as-a-service platform for advanced analytics, delivering the framework and tools necessary to provide near-real-time analysis in support of business-critical objectives. It adheres to big data best practices, uses open standards-based platforms, and integrates open source components to minimize custom development and integration, while maximizing immediate insight. Dashboard analytics feed the Cyber Hub allowing predictive decision-making.

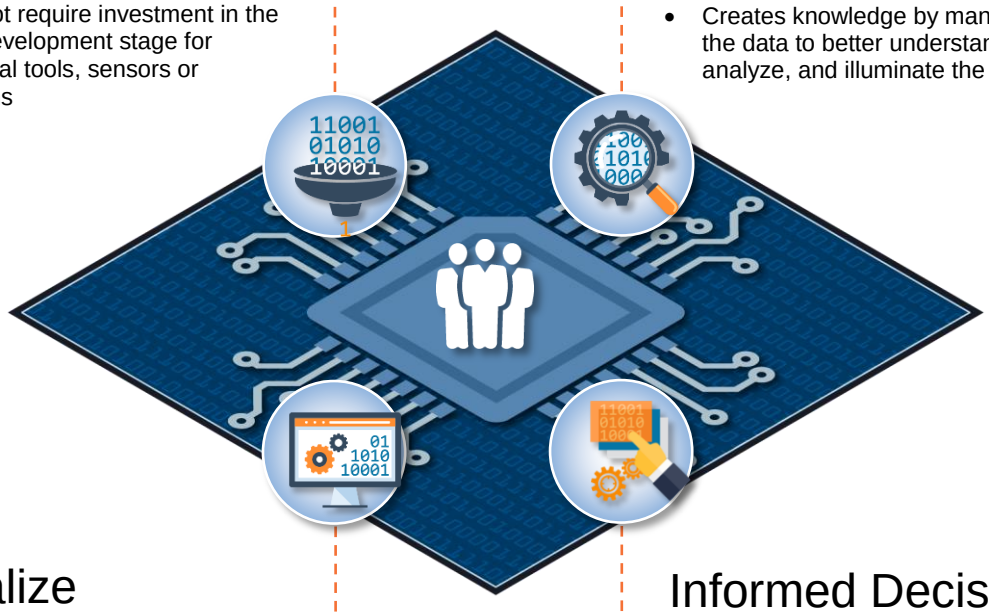
GOAL: Provide a common operating picture of the state's Cyber domain and threat environment along with the other participating states.

Data Ingest

- Infrastructure layer enabling management of existing data
- Ingests data from existing cyber management toolsets, available network sensors above and below the state managed networks, intelligence feeds, and news sources
- Does not require investment in the initial development stage for additional tools, sensors or platforms

Analyze

- Analytics layer allowing understanding of the collected data
- Compiles, compares, and analyzes data
- Applies advanced algorithms, cyber and threat analytics and state-of-the-art methodology to rapidly detect and prevent cybersecurity threats
- Creates knowledge by manipulating the data to better understand, analyze, and illuminate the problem



Visualize

- Configurable display of the aggregated and analyzed data
- Displays actionable intelligence
- Data is displayed on a map, in tables or graphics, visualizations are created that best allow decisions to be made
- True visibility of the risks to the network with focus on critical areas that require further analysis

Informed Decisions

- Application layer for leaders to make decisions upon the analyzed data and synthesized results
- Focused on key performance indicators and key risk indicators
- Allows drill down capability to get to identify the source of the problem
- Feeds the Cyber Hub Playbook allowing rapid adoption of pre-selected courses of action

This page intentionally left blank.

State Leadership Decisions

The Cyber Hub Operations Framework is dependent on four key pillars that require critical decisions and actions. Operations, Manpower, Governance, and Resources will impact the timely delivery of a functional, agile Cyber Hub.

Using current and predictive data analytics and Human-in-the-loop capabilities Hub operations will be a critical step in moving the state from a compliance based cyber security model to a risk-based model.

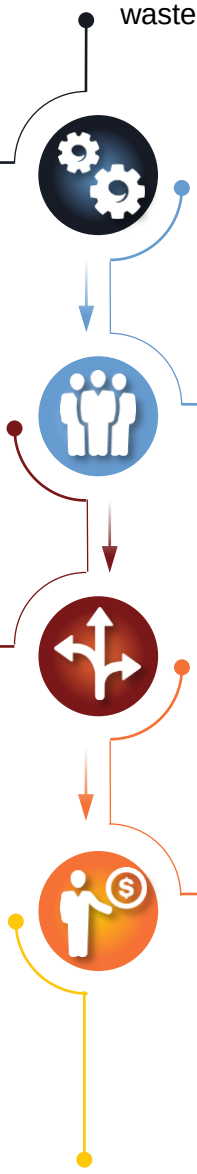
State Leadership must make decisions, based on the best available information and resources today, and most importantly remove barriers that waste time and block innovation.

Operations

- Establish Cyber Hub operating procedures for 24/7 participation by all stakeholders
- Determine decision making model for Observe, Orient, Decide, Act (OODA)
- Develop Cyber Playbook that can be continuously updated with responses across all Sectors
- Identify SCIF* mission requirements and Clearance Reciprocity processes
- Test and validate all forms of communication and collaboration on a regular schedule

Governance

- Ensure all decisions are local and accountable
- Identify stakeholders for participation and begin/continue outreach
- Develop a Charter Agreement and Memorandums of Understanding for subscribing members and stakeholders
- Engage key stakeholders to prioritize critical infrastructure cyber issues
- Establish Cyber Hub oversight roles and responsibilities
- Determine gaps in legislation and waiver requirements to existing authorities
- Define and agree upon an enterprise architecture for the cyber ecosystem



Manpower

- Establish and identify the Cyber Operations Officer (Cyber Hub Lead)
- Conduct a skill gap analysis against operational roles and responsibilities
- Identify State Government/National Guard Limiting Factors with hiring practices, the waivers that need to be employed to obtain qualified personnel, and potential legislation changes to sustain a capable cyber workforce overtime
- Identify training requirements based on skill sets and sources (in-residence and distance learning) to support qualification
- Obtain and maintain necessary clearances for cyber hub team members for SCIF access

Resources

- Correlate financial requirements and sources across the IOC-FOC timeline
- Identify facilities across the state and their relationships to the Cyber Hub
  - Co-locate key cyber team members in the Cyber Hub as soon as possible
- Determine Government employee space requirements to facilitate optimal collaboration through co-location
- Validate information technology infrastructure requirements to enable collaboration and dashboard capabilities

This page intentionally left blank.

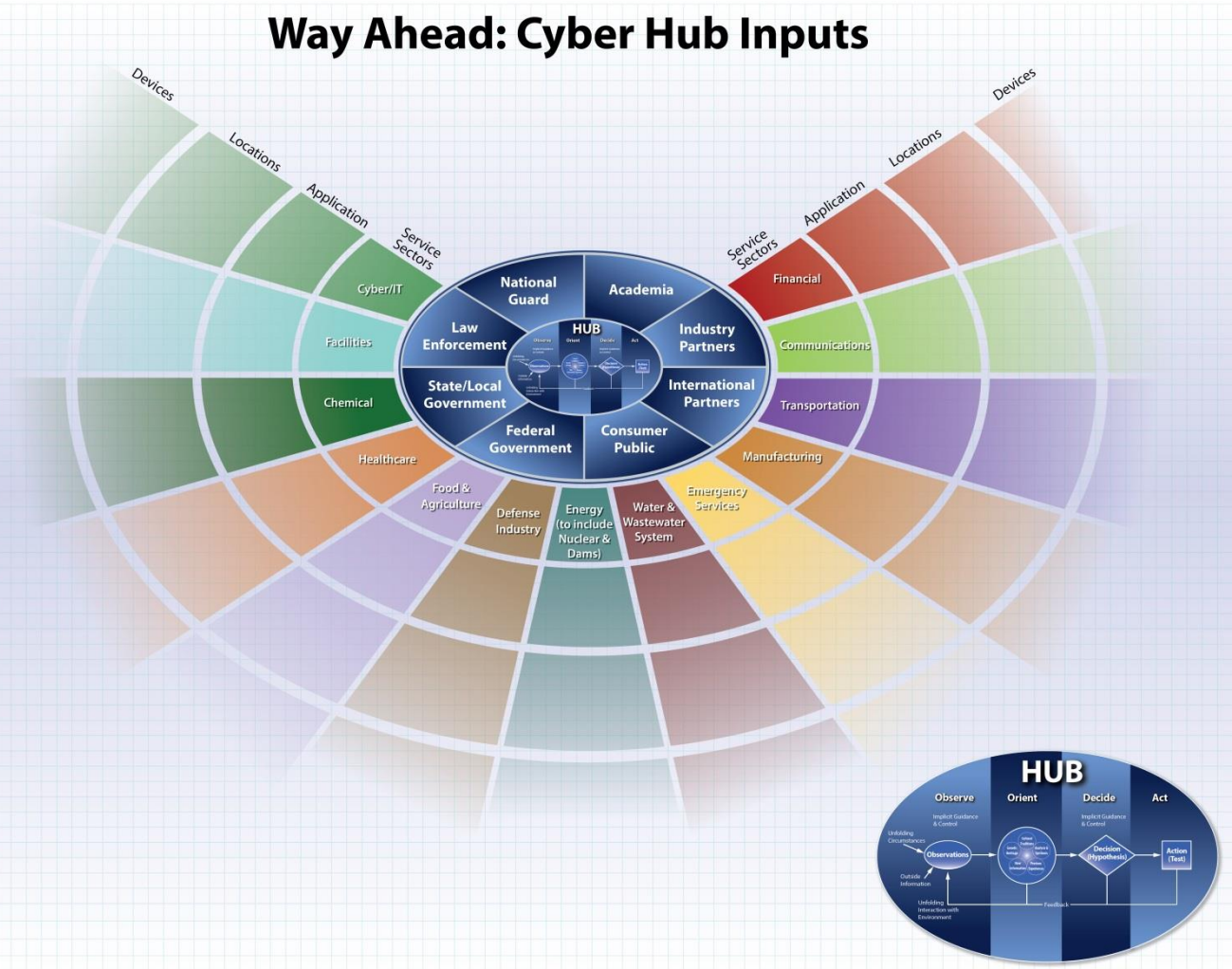
Way Ahead: Cyber Hub Inputs

Cyber Hub Inputs

The goal is to identify the relationships between the stakeholders that control their part of the Internet of Things throughout the cyber ecosystem against the cyberspace capabilities and roles within, through and across the Critical Infrastructure Sector domains. Stakeholders will need to define the breakout of cyber capabilities by application, location and type of device utilized and access controls. The cyber dashboard can then be built to provide a comprehensive visual backdrop that would show results and correlation of cyber events against an enumerated set, e.g. impacted sectors of the communication system, the power system, the water and sewage system or any other enumerated set of objects. The implicit and explicit known relationships between entities can then be mapped into the Playbook for cyber decision responses across the State's cyber ecosystem for use by Departments, Agencies, and public and private mission partners in all operational environments.

Stakeholder Responsibilities

The further development of this graphic rests with the stakeholders that participate in the launch of the Cyber hub, should the State decide to pursue the proposed model. This model will be built over time. Don't be in a hurry. Identify critical infrastructure areas first and focus on those as a matter of priority.



This page intentionally left blank.

APPENDIX F: ACRONYMS

AOA	Analysis of Alternatives
ATO	Approval to Operate
BCAs	Business Case Analyses
C2	Command and Control
CFO	Chief Financial Officer
CIO	Chief Information Officer; Command Information Officer
CMC	Cyber Hub Management Construct
CNGB	Chief of the National Guard Bureau
CNGBI	Chief of the National Guard Bureau Instruction
COA	Course(s) of Action
COBIT	Control Objectives for Information and Related Technology
CONOPS	Concept of Operations
COOP	Continuity of Operations Plan
COP	Common Operating Picture
COTS	commercial-off-the-shelf (products)
CRD	Capability Requirements Document
CS	Cybersecurity
CSP	Construction Security Plan
CTSO	Cyber Technical Synchronization Office
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DNI	Director of National Intelligence
DoD	Department of Defense
DoD CIO	Department of Defense Chief Information Officer
DoDM	Department of Defense Manual
DOJ	Department of Justice
DR	Disaster Recovery (plan)
EMS	Enterprise Management Services
EXCOM	Cyber Senior Executive Committee
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FTE	Full Time Equivalents
GOTS	government-off-the-shelf
HITL	Human-in-the-loop (process)
IC	Intelligence Community
ICD	Intelligence Community Directive
ICPG	Intelligence Community Planning Guidance
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
ISAC	Information Sharing and Analysis Center
IT	Information Technology
JFHQ	Joint Force Headquarters

JIE	Joint Information Environment
JMC	JIE Management Construct
KPI	Key Performance Indicator
LEA	Law Enforcement Agency
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NDA	Non-Disclosure Agreement
NGB	National Guard Bureau
NLP	Natural Language Processing
NTISS	National Telecommunications and Information Systems Security
OODA	Observe, Orient, Decide, Act
OPM	Office of Personnel Management
OPS	operations
POA&M	Plan of Action and Milestones
POC	Point of Contact
PPBE	Planning, Programming, Budgeting, and Execution
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SIO	State Intelligence Officer
SITREP	Situation Report
SLA	Service Level Agreement
SOP	Standard Operating Procedure
SSBI	Single Scope Background Investigation
SSM	Site Security Manager
SSO	State Security Officer
SSR	Special Security Representative
TAG	the Adjutants General
TPPs	Tactics, Techniques and Procedures
TS/SCI	Top Secret/ Sensitive Compartmental Information (clearance)
UCP	Unified Command Plan
UFC	Unified Facilities Criteria
VERDE	Visualizing Energy Resources Dynamically on Earth

APPENDIX G: DEFINITIONS

Access: Ability and means to communication with or otherwise interact with a system, to use system resources to handle information, to gain knowledge of the information the system contains, or to control system components and functions.

Accreditation: The official management decision to permit operation of an information system in a specified environment at an acceptable level of risk, based on the implementation of an approved set of technical, managerial, and procedural safeguards.

Accrediting Official: Person designated by the Cognizant Security Authority (CSA) who is responsible for all aspects of SCIF management and operations to include security policy implementation and oversight.

Agile Operations: A set of principles for operations in which requirements and solutions evolve through collaboration between self-organizing, cross-functional teams.

Algorithm: A procedure or formula for solving a problem.

Automated Response: A pre-designated reply that is generated by a software program for incoming messages.

Baseline Capabilities: A capability provides the means to accomplish a mission or function resulting from the performance of one or more critical tasks, under specified conditions, to target levels of performance. A capability may be delivered with any combination of properly planned, organized, equipped, trained, and exercised personnel that achieves the desired outcome. (Source: National Preparedness Guidelines, pg. 40) Within the context of this document, a Baseline capability for Fusion Centers is a capability necessary for the fusion center to perform its core functions of gathering, processing, analyzing, and disseminating terrorism, homeland security, and law enforcement information.

Certification: Comprehensive evaluation of the technical and non-technical security features and other safeguards, made as part of and in support of the accreditation process, to establish the extent to which a particular design and implementation meets a specified set of security requirements.

Common Operating Picture: A single identical display of relevant information shared by more than one command. A common operational picture facilitates collaborative planning and assists all echelons to achieve situational awareness.

Compartmented Area: A room, a set of rooms, or an area that provides controlled separation between compartments within a SCIF.

Compliance-based Cybersecurity: Focused primarily on the state of networks, malware, and patching. Designed to track regulations and rules on how data is managed and the need for organizations to be in compliance with these regulations.

Construction Security Plan: A plan developed by the Site Security Manager (SSM) and approved by the Authorizing/Accrediting Official, which outlines security measures to be followed to ensure security of the construction site and compliance with the SCIF construction requirements.

Cybersecurity: Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

Data Feed: A mechanism for users to receive updated data from data sources.

Data Grooming: The process of deleting old data to reduce the total database size.

Decision Support Model: A process used to support decision-making in an organization or business.

Derivative Classification: Incorporating, paraphrasing, restating, or generating in a new form information that is already classified.

Emergency Support Functions: A Grouping of government and certain private-sector capabilities into an organizational structure to provide the support, resources, program implementation, and services most likely to be needed to save lives, protect property and the environment, restore essential services and critical infrastructure, and help victims and communities return to normal, when feasible, following domestic incidents.

Fixed Facility Checklist: Standardized document used in the process of accrediting a SCIF. It documents physical, technical, and procedural security information for obtaining an initial or subsequent accreditation.

Framework: A real or conceptual structure intended to serve as a support or guide for building of something that expands the structure into something useful. In computer systems, a framework is a layered structure indicating what kind of programs can or should be build and how these programs would interrelate and interact.

Fusion Process: The overarching process of managing the flow of information and intelligence across levels and sectors of government and private industry. It goes beyond establishing an information/intelligence center or creating a computer network. The Fusion Process supports the implementation of risk-based, information-driven prevention, response, and consequence management programs. The Fusion Process turns information and intelligence into actionable knowledge.

Human-in-the-Loop: A model of computing that requires human interaction.

Incident: An occurrence, caused by either human action or natural phenomena, that requires action to prevent or minimize loss of life or damage to property and/or natural resources.

Incident Management: A comprehensive approach to pre-venting, preparing for, responding to, and recovering from terrorist attacks, major disasters, and other emergencies.

Internet of Things: A network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment.

Machine Learning: A type of artificial intelligence that provides computers with the ability to learn without being explicitly programmed, and focuses on the development of computer programs that can teach themselves to grow and change when exposed to new data.

Malware: An umbrella term used to refer to a variety of forms of hostile or intrusive software, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, scareware, and other malicious programs.

Memorandum of Understanding/Agreement: A document established between two or more parties to define their respective responsibilities in accomplishing a particular goal or mission, e.g., establishing, operating, and securing a system interconnection.

Natural Language Processing: A field of computer science, artificial intelligence, and computational linguistics concerned with the interactions between computers and human (natural) languages.

Patching: A piece of software designed to update a computer program or its supporting data in order to fix or improve it.

Proprietary Information: Material and information relating to or associated with a company's products, business, or activities, including but not limited to financial information; data or statements; trade secrets; product research and development; existing and future product designs and performance specifications; marketing plans or techniques; schematics; client lists; computer programs; processes; and know-how that has been clearly identified and properly marked by the company as proprietary information, trade secrets, or company confidential information. The information must have been developed by the company and not be available to the Government or to the public without restriction from another source.

Risk-based Cybersecurity: A model that is designed to track and assess risk to an enterprise or organization, includes a predictive capability to potentially stop impending cyber-attacks.

Risk Management: Management approach that balances the threat and vulnerabilities against the cost of security countermeasures and selects a mix of measures that provide protection without excessive cost in dollars or in the efficient flow of information to those who need it.

Security Program Plan: Formal document that provides an overview of the security requirements for an organization-wide information security program and describes the program management security controls and common security controls in place or planned for meeting those requirements.

Sensitive Compartmented Information: Classified information concerning or derived from intelligence sources, methods, or analytical processes, that is required to be handled within formal access control systems established by the Director of Central Intelligence.

Sensitive Compartmented Information Facility: Accredited area, room, group of rooms, buildings, or installation where Sensitive Compartmented Information may be stored, used, discussed, and/or processed.

Situational Awareness: the ability to identify, process, and comprehend the critical elements of information about what is happening to the team in regard to the mission.

Stakeholder: A party who contributes to, or has vested interested interest in, the outcome of an effort.

Subscribing Member: An organization that has signed a Memorandum of Understanding/ Agreement with the Cyber Hub and has payed dues for an active role within the Cyber Hub.

Supervised Machine Learning: a type of machine learning algorithm that uses a known data set (called a training data set) to make predictions. The training dataset includes input data and response values, and the algorithm seeks to build a model from these data points and make predictions of the response values for a new dataset.

TEMPEST: Refers to the investigation, study, and control of Compromising Emanations of National Security Information (NSI) from telecommunications and information processing systems.

Threat: Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system through unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Unclassified: Information that has not been determined pursuant to E.O. 12958, as amended, or any predecessor order, to require protection against unauthorized disclosure and that is not designated as classified.

Validation: Confirmation (through the provision of strong, sound, objective evidence) that requirements for a specific intended use or application have been fulfilled (e.g., a trustworthy credential has been presented, or data or information has been formatted in accordance with a defined set of rules, or a specific process has demonstrated that an entity under consideration meets, in all respects, its defined attributes or requirements).

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

1. REPORT DATE (DD-MM-YY)	2. REPORT TYPE	3. DATES COVERED (From – To)
00-06-16	Non-Standard	

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
A State Cyber Hub Operations Framework	HQ0034-14-D-0001
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBERS

6. AUTHOR(S)	5d. PROJECT NUMBER
Cameron E. DePuy, J. Corbin Fauntleroy, Andrew S. Ferguson Robert M. Rolfe	BK-5-3889
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESSES	8. PERFORMING ORGANIZATION REPORT NUMBER
Institute for Defense Analyses 4850 Mark Center Drive Alexandria, VA 22311-1882	NS D-8008 H 2016-000625

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR'S / MONITOR'S ACRONYM
Kevin Garrison Principal Director/Director Analytics, Office of the Secretary of Defense, Chief Information Officer The Pentagon, Rm. 3B1056	OSD CIO
	11. SPONSOR'S / MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

Project Leader: Laura A. Odell

14. ABSTRACT

Over the last decade, the cybersecurity landscape has changed dramatically. Cybersecurity concerns are now center stage at all levels of industry, government, and the law enforcement and emergency services communities. While progress has been made in efforts to gather and share intelligence, data, and information, a significant gap remains between the ability to gather and share information and the ability to predict impending cyber-attacks and to thwart them before they are successful. The Cyber Hub Operations Framework was created to support collaboration and cooperation among a wide range of stakeholders. This framework is intended to leverage, not replace, existing organizations and structures, and move states toward an operational cyber construct that is risk-based versus compliance-based.

15. SUBJECT TERMS

Cybersecurity, Decision Support

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Kevin Garrison
Unclassified	Unclassified	Unclassified	Unlimited	68	19b. TELEPHONE NUMBER (Include Area Code) 703-614-2778